

Microsoft Dynamics™ GP

Sicherheitsplanung

Veröffentlichungsdatum

Oktober 2005

Inhalt

Einführung

Verwenden Sie die Informationen in diesem Dokument, um die Sicherheit in Microsoft Dynamics GP zu planen.

Diese Einführung ist in folgende Abschnitte unterteilt:

- *Inhalt dieses Dokuments*
- *Symbole und Konventionen*
- *Senden Sie Ihre Kommentare zur Dokumentation*

Inhalt dieses Dokuments

Dieses Dokument soll Sie mit Verfahren vertraut machen, die Sie durchführen können, um Ihre Microsoft Dynamics GP-Daten so sicher wie möglich zu machen.

Microsoft Windows®, die Grundlage von Microsoft Dynamics GP, bietet eine komplexe, auf Standards basierende Netzwerksicherheit. Letztlich geht es bei der Sicherheit um das Planen und Erwägen von Kompromissen. So kann beispielsweise ein Computer in einem Tresorraum versperrt und nur für einen Systemadministrator zugänglich sein. Dieser Computer mag zwar sicher, jedoch nicht ausreichend nutzbar sein, da er mit keinem anderen Computer verbunden ist. Sie müssen also entscheiden, wie das Netzwerk so sicher wie möglich gemacht werden kann, ohne dabei dessen Verwendbarkeit zu beeinträchtigen.

Die meisten Organisationen planen im Hinblick auf externe Angriffe und verwenden Firewalls, bedenken jedoch häufig nicht, was geschehen soll, wenn ein bösartiger Benutzer über eine Sicherheitslücke die Firewall überwindet. Die Sicherheitsmaßnahmen Ihrer Organisation werden dann gut funktionieren, wenn die Benutzer für ein sicheres Erledigen ihrer Arbeit nicht allzu viele Prozeduren und Schritte durchführen müssen. Das Implementieren von Sicherheitsrichtlinien sollte für die Benutzer so einfach wie möglich sein, da diese ansonsten dazu neigen, weniger sichere Methoden vorzuziehen.

Da die Größe einer Implementierung von Microsoft Dynamics GP sehr unterschiedlich sein kann, ist es wichtig, die Anforderungen eines kleineren Unternehmens sorgfältig abzuwägen, insbesondere hinsichtlich des Verhältnisses von Effektivität und Kosten. Empfehlen Sie mit Bedacht eine Richtlinie, die die Sicherheitsanforderungen erfüllt.

Dieses Dokument ist in folgende Abschnitte unterteilt:

- Kapitel 1, „Grundlegende Sicherheitsempfehlungen“, erläutert einige grundlegende Sicherheitsempfehlungen, die Ihnen dabei helfen sollen, Ihre Microsoft Dynamics GP-Daten so sicher wie möglich zu machen.

- Kapitel 2, „Sichern des Serverbetriebssystems“, beinhaltet Informationen zum Sichern des Serverbetriebssystems.

- Kapitel 3, „Netzwerksicherheit“, beinhaltet Informationen zum Sichern Ihres Netzwerks.

- Kapitel 4, „Virenschutz“, bietet Informationen zu den verschiedenen Virustypen sowie Maßnahmen für den Schutz Ihres Computers vor einer Infektion mit einem Virus.

- Kapitel 5, „Microsoft Dynamics GP Sicherheit“, beinhaltet eine Übersicht der in Microsoft Dynamics GP enthaltenen Sicherheitsfeatures.
- Kapitel 6, „Das Microsoft Dynamics GP-Datenbanksicherheitsmodell“, enthält Informationen zum Microsoft Dynamics GP-Datenbanksicherheitsmodell.
- Kapitel 7, „Sicherheitsaufgaben für Hauptanwendungen“, listet die sichersten Optionen zum Ausführen allgemeiner Sicherheitsaufgaben in Microsoft Dynamics GP auf.
- Kapitel 8, „Häufig gestellte Fragen“, beinhaltet Antworten auf häufig gestellte Fragen zur Sicherheit in Microsoft Dynamics GP.

Symbole und Konventionen

In diesem Dokument werden folgende Symbole verwendet, um Sie auf Informationen aufmerksam zu machen.

Symbol	Beschreibung
	Das Glühbirnensymbol weist auf hilfreiche Tipps, Verknüpfungen und Vorschläge hin.
	Das Warnsymbol macht auf Situationen aufmerksam, auf die Sie besonders achten sollten.

In diesem Dokument werden die folgenden Konventionen verwendet, um auf Abschnitte, Navigationsmöglichkeiten oder andere Informationen zu verweisen.

Konvention	Beschreibung
Erstellen eines Stapels	Kursivschrift kennzeichnet den Namen eines Abschnitts oder einer Prozedur.
Datei >> Drucken oder **Datei > Drucken**	Das Symbol (>>) oder (**>**) kennzeichnet eine Reihe aufeinander folgender Aktionen, z. B. das Auswählen von Elementen aus einem Menü oder einer Symbolleiste oder das Klicken auf Schaltflächen in einem Fenster. In diesem Beispiel soll im Menü „Datei“ der Befehl „Drucken“ ausgewählt werden.
REGISTERKARTE oder EINGABETASTE	Großbuchstaben dienen zur Bezeichnung von Tasten oder Tastenkombinationen.

Senden Sie Ihre Kommentare zur Dokumentation

Kommentare zur Nützlichkeit der Microsoft Dynamics GP-Dokumentation sind jederzeit willkommen. Wenn Sie Vorschläge oder Anmerkungen zu diesem Dokument machen möchten, senden Sie diese per E-Mail an folgende Adresse: bizdoc@microsoft.com.

Um Kommentare zu bestimmten Hilfethemen zu senden, klicken Sie auf den Link „Feedback zur Dokumentation“, der sich am unteren Rand des jeweiligen Hilfethemas befindet.

Hinweis: Indem Sie Microsoft® Ihre Vorschläge anbieten, geben Sie Microsoft die volle Berechtigung, sie frei zu verwenden.

Kapitel 1: Grundlegende Sicherheitsempfehlungen

Vor dem Einrichten von Microsoft Dynamics GP ist die Auseinandersetzung mit den folgenden Sicherheitsempfehlungen sinnvoll.

Die Informationen sind in folgende Abschnitte unterteilt:

Für eine sichere Installation von Microsoft Dynamics GP müssen die folgenden Schritte beachtet werden:



Zum Ausführen einer sicheren Microsoft Dynamics GP-Umgebung ist die Einrichtung einer sicheren Kommunikation zwischen dem Microsoft Dynamics GP-Client und SQL Server erforderlich. Wenn die Installation von Microsoft Dynamics GP nicht unter Berücksichtigung dieser Richtlinien erfolgt, ist das Programm möglicherweise anfällig für schwerwiegende Sicherheitsrisiken.

Für Microsoft SQL Server 2000 müssen Zertifikate mit dem SSL-Protokoll (SSL – Secure Sockets Layer) verwendet werden, damit die Kommunikationsverbindung zwischen dem Microsoft Dynamics GP-Client und Microsoft SQL Server 2000 gewährleistet werden kann. Wenn Sie SQL Server für SSL konfigurieren, müssen alle zwischen Client und Server übertragenen Daten verschlüsselt werden, damit die Datenübertragung zwischen Client und SQL Server sicher erfolgen kann. Wenn Sie derzeit keine SSL-Zertifikate verwenden, müssen Sie diese bei Microsoft Certificate Services anfordern.

Es wird außerdem empfohlen, den Anweisungen im Handbuch von Microsoft SQL Server 2000 Books Online zu folgen, damit die Kommunikationsverbindung zwischen SQL Server und dem Clientcomputer gewährleistet werden kann.

Microsoft SQL Server 2005 verschlüsselt standardmäßig die Übertragung der Anmeldeinformationen. Damit jedoch die Kommunikation zwischen SQL Server 2005 und Microsoft Dynamics GP während der gesamten Sitzung verschlüsselt erfolgen kann, müssen Sie den Anweisungen im Handbuch von Microsoft SQL Server 2000 Books Online folgen.

Weitere Information zur Netzwerksicherung finden Sie auf den folgenden Websites:

Sichern des Datenzugriffs
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetch12.asp

Verschlüsseln der gesamten Kommunikation zwischen Client und Server mithilfe von SSL-Zertifikaten
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetht19.asp

Verwenden von Microsoft SQL Server 2005
http://www.microsoft.com/sql/2005/default.mspx

Zum Ausführen einer sicheren Microsoft Dynamics GP-Umgebung sollten Sie einige allgemeine Administrationsregeln beachten:

- Wenn der Inhaber oder Geschäftsführer einer Firma über Administratorrechte verfügt, müssen diese Berechtigungen über die Domäne beispielsweise nicht an Kreditoren-Sachbearbeiter, Kassierer oder Verkäufer vergeben werden. Auf diese Benutzerkonten sollten nur Domänenbenutzer Zugriff haben.

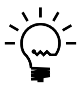
- Gleiche Passwörter sollten nicht mehrfach verwendet werden. Häufig werden Passwörter system- und domänenübergreifend wiederverwendet. Ein für zwei Domänen zuständiger Administrator erstellt beispielsweise in jeder Domäne Domänenadministratorkonten mit demselben Passwort und legt sogar auf Domänencomputern lokale Administratorpasswörter fest, die für die gesamte Domäne identisch sind. In diesem Fall kann die Kompromittierung eines einzelnen Kontos oder Computers zu einer Gefährdung der gesamten Domäne führen.

- Domänenadministratorkonten sollten nicht als Dienstkonten verwendet werden. Häufig werden Domänenadministratorkonten auch als Dienstkonten für allgemeine Dienste wie z. B. der Systemsicherung eingerichtet. Daraus ergibt sich jedoch ein Sicherheitsrisiko, da das Passwort lokal auf jedem Computer, der diesen Dienst verwendet, gespeichert oder zwischengespeichert werden muss. Das Passwort kann dann problemlos von jedem Benutzer abgerufen werden, der über Administratorrechte für diesen Computer verfügt. Auch in diesem Fall kann die Kompromittierung eines einzelnen Computers zu einer Gefährdung der gesamten Domäne führen. Dienstkonten sollten nie als Domänenadministratorkonto festgelegt werden. Außerdem sollten die Berechtigungen für Dienstkonten möglichst nur eingeschränkt vergeben werden.

- Obwohl Microsoft Dynamics GP von mehreren Betriebssystemen unterstützt wird, sollte vorzugsweise das neueste Betriebssystem mit den aktuellen Sicherheitsfeatures verwendet werden. Für Firmenzwecke vorgesehene Versionen von Betriebssystemen verfügen zudem normalerweise über zusätzliche Sicherheitsfeatures.

- Um die aktuellen Sicherheitspatches zu verwalten, sollte das Windows Update-Tool von Windows 2000, Windows XP und Windows Server 2003 verwendet werden.

- Wenn Sie Microsoft Dynamics GP Business Portal verwenden möchten, sollten Sie die im Business Portal-Installationshandbuch aufgeführten Sicherheitsempfehlungen implementieren. Das Handbuch ist auf der CustomerSource-Website erhältlich.



Die verbleibenden Abschnitte dieses Dokuments enthalten Empfehlungen zu verschiedenen Methoden der Sicherheitsoptimierung der Microsoft Dynamics GP-Installation. Diese Empfehlungen sollten unbedingt beachtet werden, müssen jedoch nicht umgesetzt werden.

Physische Sicherheit

Die physische Sicherheit ist die Voraussetzung für die Abwehr bösartiger Angriffe. Wenn beispielsweise ein Festplattenlaufwerk entwendet wird, werden auch die

darauf befindlichen Daten gestohlen. Bringen Sie bei der Ausarbeitung von Richtlinien die folgenden Problembereiche bezüglich der physischen Sicherheit zur Sprache:

- Bei umfangreicheren Einrichtungen mit eigenen IT-Abteilungen sollten Serverräume sowie Orte, an denen Software und Handbücher gelagert werden, verschlossen werden.
- Verhindern Sie den Zugang nicht berechtigter Benutzer zu Netzschalter und Resettaste des Servers.
- Ziehen Sie das Entfernen jeglicher Wechselmedien-Geräte (auch CD-Brenner) aus Client-Workstations in Betracht.
- Installieren Sie unabhängig von der Vertraulichkeit der Daten eine Alarmanlage.
- Achten Sie darauf, dass Sicherungskopien wichtiger Daten außerhalb und Softwarekopien in feuer- und wasserfesten Behältern gelagert werden.

Mitarbeiter

Die Vergabe von Administratorrechten sollte für sämtliche Produkte und Features nur eingeschränkt erfolgen. Standardmäßig sollten die Mitarbeiter nur schreibgeschützten Zugriff auf Systemfunktionen erhalten, es sei denn, sie benötigen den erweiterten Zugriff zur Ausübung ihrer Tätigkeit. Microsoft empfiehlt grundsätzlich die Einhaltung der „Regel der geringsten Rechte“: Erteilen Sie den Benutzern nur die für den Datenzugriff und den Erhalt der Funktionalität erforderlichen Rechte. Zum Ausführen von Features sollten keine Administratorrechte erforderlich sein.

Verärgerte und ehemalige Mitarbeiter können eine Bedrohung der Netzwerksicherheit darstellen. Die Verwendung folgender Mitarbeiterrichtlinien hat sich als erfolgreich erwiesen:

- Überprüfen Sie vor der Einstellung den Hintergrund des Mitarbeiters.
- Sie müssen immer mit eventuellen „Rachegelüsten“ verärgerter und ehemaliger Mitarbeiter rechnen.
- Bei Ausscheiden eines Mitarbeiters aus dem Unternehmen sollten alle ihm zugeordneten Windows-Konten und Passwörter deaktiviert werden. Löschen Sie die Benutzer jedoch nicht, damit Sie weiterhin Berichte erstellen können.
- Schulen Sie die Benutzer hinsichtlich der Erkennung und Meldung verdächtiger Vorgänge.
- Gewähren Sie Berechtigungen nicht automatisch. Verhindern Sie den Zugriff auf bestimmte Computer, Computerräume oder Dateien, wenn Benutzer diese nicht benötigen.
- Schulen Sie Vorgesetzte im Hinblick auf Erkennung von und Umgang mit potenziellen Mitarbeiterproblemen.
- Überwachen Sie die Systemverwendung in Bezug auf ungewöhnliche Aktivitäten.

- Machen Sie den Mitarbeitern ihre Verantwortung für die Netzwerksicherheit bewusst.
- Händigen Sie jedem Mitarbeiter ein Exemplar der Firmenrichtlinien aus.
- Untersagen Sie den Benutzern die Installation eigener Software.

Systemadministratoren

Systemadministratoren sollten bezüglich der aktuellen bei Microsoft verfügbaren Sicherheitsfixes informiert sein. Hacker sind sehr versiert darin, durch die Kombination kleinerer Programmfehler umfangreiche Eingriffe in ein Netzwerk zu bewerkstelligen. Administratoren sollten zunächst die einzelnen Computer soweit wie möglich sichern und danach verfügbare Sicherheitsupdates und -patches installieren. In dieser Hinsicht können die zahlreichen in diesem Handbuch enthaltenen Links und Ressourcen bei der Suche nach sicherheitsrelevanten Informationen und bewährten Methoden Unterstützung bieten.

Die Komplexität eines Netzwerks kann dessen Sicherung erschweren. Je komplexer ein Netzwerk aufgebaut ist, desto schwieriger gestaltet sich häufig nach dem erfolgreichen Zugriff durch Angreifer die Sicherung oder die Reparatur. Der Administrator sollte die Netzwerktopografie ausführlich und möglichst plausibel dokumentieren.

Die Sicherung beinhaltet in hohem Maße auch Risikomanagement. Die Verwendung von Technologien allein reicht zur Gewährleistung der Sicherheit nicht aus. Eine erfolgreiche Sicherung erfordert die Kombination von Technologien und klaren Richtlinien. Das heißt, die Sicherheit ist letztlich stark davon abhängig, wie die verfügbaren Technologien eingesetzt werden. Microsoft stellt Technologien und Features für die Sicherheit zur Verfügung. Nur der Administrator und das Management können jedoch die individuell erforderlichen Richtlinien für jedes Unternehmen festlegen. Planen Sie die Sicherheit schon in den frühen Implementierungs- und Bereitstellungsphasen. Machen Sie sich damit vertraut, welche Informationen Ihre Firma schützen möchte und welche Mittel Sie zu deren Schutz einsetzen können.

Erarbeiten Sie zudem Kontingenzpläne für Notfälle, bevor diese auftreten, und verbinden Sie dabei eine gründliche Planung mit zuverlässigen Technologien. Weitere Informationen zur allgemeinen Sicherheit finden Sie in englischer Sprache im Artikel „The Ten Immutable Laws of Security Administration“ unter http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

Verwalten von Sicherheitspatches

Betriebssysteme und Anwendungen zeichnen sich häufig durch ihre hohe Komplexität aus. Sie können aus Millionen von Codezeilen bestehen, die von vielen verschiedenen Programmierern entwickelt wurden. Die Software muss absolut zuverlässig funktionieren und darf die Sicherheit oder Stabilität der IT-Umgebung nicht gefährden. Vor der Veröffentlichung werden die Programme gründlich getestet, damit beim Ausführen nach Möglichkeit keine Probleme auftreten. Da Hacker jedoch kontinuierlich nach Schwachstellen in der Software suchen, ist es nicht möglich, potenzielle zukünftige Angriffe im Voraus zu erkennen.

In vielen Unternehmen wird die Verwaltung von Sicherheitspatches zum Teil der allgemeinen Managementstrategie hinsichtlich der Änderungen und

Konfigurationen. Unabhängig von Art und Größe des Unternehmens ist jedoch eine durchdachte Strategie zur Patchverwaltung erforderlich – auch wenn das Unternehmen noch nicht über eine erfolgreiche Änderungs- und Konfigurationsmanagementstrategie verfügt. Die meisten erfolgreichen Angriffe gegen Computer erfolgen bei Systemen ohne installierte Sicherheitspatches.

Sicherheitspatches stellen für viele Unternehmen eine besondere Herausforderung dar. Wenn bei einer Software eine Schwachstelle entdeckt wurde, verbreiten sich diesbezügliche Informationen unter Hackern normalerweise sehr schnell. Tritt bei einer Software eine Schwachstelle auf, versucht Microsoft umgehend, einen Sicherheitspatch zu veröffentlichen. Bis zur Bereitstellung des Patches kann allerdings die vom Benutzer benötigte und erwartete Sicherheit nicht gewährleistet werden.

In einer Windows-Umgebung müssen jeweils die aktuellen Sicherheitspatches im gesamten System verfügbar sein. Zum Erreichen dieses Ziels sollten Sie die Verwendung der von Microsoft dafür zur Verfügung gestellten Technologien in Betracht ziehen. Dazu gehören beispielsweise:

Microsoft Security Notification Service Sobald Aktualisierungen zur Verfügungen stehen, sendet der Security Notification Service automatisch per E-Mail eine Benachrichtigung. Diese Benachrichtigungen sind wichtiger Bestandteil einer aktiven Sicherheitsstrategie. Diese Benachrichtigungen stehen auch unter folgendem Link auf der TechNet Product Security Notification-Website zur Verfügung: http://www.microsoft.com/technet/security/bulletin/notify.mspx.

Suchtool für Microsoft-Sicherheitsbulletins Das Suchtool für Microsoft-Sicherheitsbulletins kann auf der Website für Hotfixes und Sicherheitsbulletins abgerufen werden. Sie können entsprechend den von Ihnen verwendeten Betriebssystemen, Anwendungen und Service Packs festlegen, welche Aktualisierungen Sie benötigen. Weitere Information über das Suchtool für Microsoft-Sicherheitsbulletins finden Sie unter http://www.microsoft.com/technet/security/current.aspx.

Microsoft Baseline Security Analyzer (MBSA) Dieses Tool mit grafischer Oberfläche steht auf der Microsoft Baseline Security Analyzer-Website zur Verfügung. Dieses Tool vergleicht den aktuellen Status eines Computers mit den bei Microsoft verfügbaren Aktualisierungen. MBSA führt zudem grundlegende Sicherheitsüberprüfungen bezüglich der Passwortsicherheit und der Einstellungen für das Ablaufdatum sowie zu Richtlinien für Gastkonten und anderen Bereichen durch. Außerdem sucht MBSA nach Schwachstellen von Microsoft-Internetinformationsdiensten (IIS – Internet Information Services), Microsoft SQL Server™ 2000, Microsoft Exchange 5.5, Microsoft Exchange 2000 und Microsoft Exchange Server 2003. Weitere Information über MBSA erhalten Sie unter http://www.microsoft.com/technet/security/tools/mbsahome.mspx.

Microsoft Software Update Services (SUS) Dieses Tool (früher Windows Update Corporate Edition) ermöglicht Unternehmen die Bereitstellung aller wichtigen auf der öffentlichen Windows Update-Website zur Verfügung stehenden Aktualisierungen und Sicherheits-Rollup-Pakete (SRPs). Das Tool bietet unter Verwendung neuer Versionen der Clients für automatische Updates (AU) die Grundlage für eine leistungsfähige Strategie zum automatischen Download und zur Installation. Die neuen AU-Clients beinhalten einen Client für die Betriebssysteme Windows 2000 und Windows Server 2003, der automatisch die heruntergeladenen Updates installiert. Weitere Information über Microsoft SUS

finden Sie unter http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

Microsoft Systems Management Server (SMS) Software Update Services Feature Pack Das SMS Software Update Services Feature Pack enthält mehrere Tools, die den Vorgang der Bereitstellung von Softwareaktualisierungen innerhalb des Unternehmens erleichtern. Dazu gehören ein Security Update Inventory Tool, ein Microsoft Office Inventory Tool für Updates, der Assistent für die Verteilung von Softwareaktualisierungen sowie ein SMS Web Reporting Tool mit dem Add-In für Webberichte zu Softwareaktualisierungen. Weitere Informationen zu den einzelnen Tools finden Sie unter http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Es wird empfohlen, diese Sicherheitstools zu verwenden. Sicherheitsprobleme sollten so schnell wie möglich gelöst werden, während gleichzeitig die Stabilität der Umgebung gewährleistet sein muss.

Microsoft Dynamics GP Service Packs

Microsoft Dynamics GP-Sicherheitspatches werden in Service Packs veröffentlicht. Service Packs sind auf der CustomerSource-Website im Bereich „Downloads and Updates" verfügbar. Sie sollten diese Seite regelmäßig auf Aktualisierungen überprüfen, sodass Sie über Sicherheitsprobleme von Microsoft Dynamics GP informiert sind. Aktuelle Anweisungen zum Upgrade auf die jeweils neueste Version von Microsoft Dynamics GP finden Sie unter http://mbs.microsoftt.com/public/gponline.

Clientbasierte Sicherheitspatches

Benutzer von Microsoft Dynamics GP können den neuesten Stand ihrer Clientcomputer bezüglich verfügbarer Sicherheitspatches für Microsoft Windows 2000, Windows XP und Windows Server 2003 gewährleisten, indem sie die Windows Update-Funktion der Betriebssysteme verwenden. Wenn Microsoft Security Update Services auf dem Server installiert sind, kann die Aktualisierung intern durch die IT-Abteilung des Unternehmens weitgehend automatisiert werden. Der Microsoft Security Notification Service sendet ausführliche Informationen zu allen Sicherheitspatches für SQL Server 2000.

Kapitel 2: Sichern des Serverbetriebssystems

Im Folgenden finden Sie einige der bewährten Verfahrensweisen zur Sicherung von Serverbetriebssystemen. Diese Informationen sollten vor der Implementierung von Microsoft Dynamics GP berücksichtigt werden.

Die Informationen sind in folgende Abschnitte unterteilt:

Sicherheit des Serverbetriebssystems

Kleinere Unternehmen verfügen oftmals nicht über ein Serverbetriebssystem. Dennoch ist es für die Manager solcher Unternehmen wichtig, mit einem Großteil der bewährten Verfahrensweisen zur Sicherung vertraut zu sein, die auch auf größere Unternehmen mit komplexeren Netzwerkumgebungen anwendbar sind. Beachten Sie, dass viele der Richtlinien und Verfahrensweisen in diesem Dokument leicht auf Unternehmen mit nur einem Clientbetriebssystem übertragbar sind.

Die Konzepte in diesem Abschnitt beziehen sich auf die Produkte Microsoft Windows 2000 Server und Microsoft Windows Server™ 2003, wobei die Informationen hauptsächlich aus der Onlinehilfe von Windows Server 2003 stammen. Windows Server 2003 bietet umfangreiche Sicherheitsfunktionen. In der Onlinehilfe von Windows Server 2003 sind ausführliche Informationen zu allen Sicherheitsfunktionen und -verfahren enthalten.

Weitere Informationen zu Windows 2000 Server finden Sie im Windows 2000 Server-Sicherheitscenter unter http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx (in englischer Sprache).

Für Windows Server 2003 wurde von Microsoft das „Sicherheitshandbuch für Windows Server 2003“ herausgegeben, das Sie unter http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx finden.

Die wichtigsten Funktionen des Windows-Sicherheitsmodells für Server sind Authentifizierung, Zugriffssteuerung und einmaliges Anmelden, wie im Folgenden erläutert wird.

- Authentifizierung beschreibt den Vorgang, bei dem die Identität eines Benutzers mithilfe der Anmeldeinformationen vom System überprüft wird. Benutzername und Passwort werden mit einer Liste autorisierter Benutzer verglichen. Wenn das System eine Übereinstimmung erkennt, wir der Zugriff in dem Umfang gewährt, der in der Berechtigungsliste für diesen Benutzer festgelegt ist.

- Durch Zugriffssteuerung wird der Zugriff des Benutzers auf Informationen oder Ressourcen auf Grundlage der Identität des Benutzers und seiner Mitgliedschaft in verschiedenen vordefinierten Gruppen beschränkt. Zugriffssteuerung wird üblicherweise von Systemadministratoren verwendet, um den Benutzerzugriff auf Netzwerkressourcen wie Server, Verzeichnisse und Dateien zu steuern. Sie wird normalerweise durch die Zuteilung von Berechtigungen an Benutzer und Gruppen für bestimmte Objekte implementiert.

- Durch einmaliges Anmelden kann sich ein Benutzer mit einem einzigen Kennwort einmalig an der Windows-Domäne anmelden und authentifiziert sich somit an allen Computern in der Windows-Domäne. Durch die einmalige Anmeldung haben Administratoren die Möglichkeit, eine sichere Kennwortauthentifizierung im gesamten Windows-Netzwerk zu implementieren, während der Zugriff für Benutzer vereinfacht wird.

Die folgenden Themen enthalten eine ausführlichere Beschreibung dieser drei Schlüsselfunktionen zur Sicherung Ihrer Computerumgebung.

Authentifizierung

Authentifizierung ist ein grundlegender Aspekt der Sicherheit des Systems. Durch Authentifizierung wird die Identität von Benutzern bestätigt, die sich an einer Domäne anmelden oder auf Netzwerkressourcen zugreifen möchten. Das schwache Glied in jedem Authentifizierungssystem ist das Passwort des Benutzers.

Passwörter stellen die erste Verteidigungshürde gegen nicht autorisierten Zugriff auf die Domäne und lokale Computer dar. Wir empfehlen die Verwendung bewährter Verfahrensweisen für Passwörter in Ihrer Organisation, sofern dies möglich ist. Weitere Informationen finden Sie unter *Passwortschutz* auf Seite 10, *Sichere Passwörter* auf Seite 11 und *Festlegen der Passwortrichtlinie* auf Seite 13.

Passwortschutz

Es ist immer wichtig, dass Benutzer Passwörter verwenden und diese Empfehlungen beachten.

- Lassen Sie nur sichere Passwörter zu. Weitere Informationen finden Sie unter *Sichere Passwörter* auf Seite 11.

- Wenn Passwörter aufgeschrieben werden müssen, bewahren Sie das Papier an einem sicheren Ort auf, und vernichten Sie es, wenn es nicht mehr benötigt wird.

- Teilen Sie Passwörter niemals anderen Personen mit.

- Verwenden Sie für alle Benutzerkonten verschiedene Passwörter.

- Ändern Sie Passwörter umgehend, wenn diese offen gelegt wurden.

- Achten Sie darauf, wo Sie Passwörter auf Computern speichern. Einige Dialogfelder, wie solche für den Remotezugriff und andere Telefonverbindungen, bieten die Option, ein Passwort zu speichern. Die Auswahl dieser Option stellt ein Sicherheitsrisiko dar, da das Passwort in der Systemregistrierung gespeichert wird.

Sichere Passwörter

Die Bedeutung von Passwörtern bei der Sicherung des Netzwerks in einer Organisation wird oft unterschätzt. Wie bereits erwähnt, stellen Passwörter die erste Verteidigungshürde gegen nicht autorisierten Zugriff auf Ihre Organisation dar. Die Windows Server 2003-Produktfamilie enthält eine neue Funktion, mit der die Komplexität des Passworts für das Administratorkonto während der Installation des Betriebssystems kontrolliert wird. Wenn das Passwort leer ist oder den Komplexitätsvoraussetzungen nicht entspricht, wird ein Windows Setup-Dialogfeld mit dem Hinweis auf die Gefahren angezeigt, die durch das Fehlen eines sicheren Passworts für das Administratorkonto entstehen.

In einer Arbeitsgruppenumgebung kann ein Benutzer nicht über das Netzwerk auf einen Computer zugreifen, wenn ein Konto mit einem leeren Passwort verwendet wird. Durch unsichere Passwörter können Angreifer leicht auf die Computer und das Netzwerk zugreifen, während sichere Passwörter wesentlich schwieriger zu entschlüsseln sind, auch wenn dazu entsprechende Software verwendet wird, die heutzutage verfügbar ist.

Tools zum Entschlüsseln von Passwörtern werden fortwährend verbessert, und die dafür verwendeten Computer sind so leistungsstark wie nie. Bei Software zum Entschlüsseln von Passwörtern wird einer von drei Ansätzen verwendet: Intelligentes Raten, Wörterbuchangriffe und automatisierte Brute-Force-Angriffe, bei denen jede mögliche Zeichenkombination getestet wird. Bei ausreichender Zeit kann mit der automatisierten Methode jedes Passwort entschlüsselt werden. Dennoch sind sichere Passwörter viel schwieriger zu entschlüsseln als unsichere Passwörter. Ein sicherer Computer verfügt über sichere Passwörter für alle Benutzerkonten.

Ein unsicheres Passwort

- Ist so gut wie kein Passwort.
- Enthält den Benutzernamen, den echten Namen oder den Namen des Unternehmens.
- Enthält ein vollständiges Wort aus dem Wörterbuch. Beispielsweise ist „Passwort“ ein unsicheres Passwort.

Ein sicheres Passwort

- Besteht aus mindestens sieben Zeichen.
- Enthält nicht den Benutzernamen, den echten Namen oder den Namen des Unternehmens.
- Enthält kein vollständiges Wort aus dem Wörterbuch.
- Unterscheidet sich maßgeblich von vorherigen Passwörtern. Passwörter mit aufsteigender Zahl (Passwort1, Passwort2, Passwort3...) sind nicht sicher.

- Enthält Zeichen aus allen in der folgenden Tabelle aufgelisteten vier Gruppen.

Gruppe	Beispiel
Großbuchstaben	A B C D
Kleinbuchstaben	a b c d
Ziffern	0 1 2 3 4
Symbole	‘ ~ @ # $ % ^ & * ( ) _ + - = { } [ ] \ : “ ; < > ? , . /

Beispiele für ein sicheres Passwort sind „Pa$sw0rT“ und „J*p2le04>F“.

Ein Passwort kann die meisten Kriterien für ein sicheres Passwort erfüllen und trotzdem vergleichsweise unsicher sein. Beispielsweise ist „Hello2U!“ ein eher unsicheres Passwort, obwohl fast alle Kriterien für ein sicheres Passwort und die Komplexitätsvoraussetzungen der Passwortrichtlinie erfüllt sind. „H!elZl2o“ ist ein sicheres Passwort, da das Wort aus dem Wörterbuch mit Symbolen, Ziffern und anderen Buchstaben durchsetzt ist. Es ist wichtig, alle Benutzer über die Vorteile sicherer Passwörter in Kenntnis zu setzen und sie darüber zu informieren, wie ein wirklich sicheres Passwort ausgewählt wird.

Passwörter können Zeichen aus dem erweiterten ASCII-Zeichensatz enthalten. Durch die Verwendung dieses Zeichensatzes können Benutzer die Anzahl der möglichen Zeichen bei der Wahl Ihres Passworts erhöhen. Software zum Entschlüsseln von Passwörtern benötigt wahrscheinlich mehr Zeit zum Entschlüsseln von Passwörtern mit erweiterten ASCII-Zeichen als für andere Passwörter. Überprüfen Sie sorgfältig, ob Passwörter mit erweiterten ASCII-Zeichen mit anderen in Ihrer Organisation verwendeten Anwendungen kompatibel sind, bevor Sie diese einsetzen. Seien Sie besonders vorsichtig bei der Verwendung von erweiterten ASCII-Zeichen in Passwörtern, wenn in der Organisation verschiedene Betriebssysteme verwendet werden.

Erweiterte ASCII-Zeichen finden Sie in der Zeichentabelle. Einige dieser erweiterten ASCII-Zeichen sollten nicht in Passwörtern verwendet werden. Verwenden Sie ein Zeichen nicht, wenn dafür in der unteren rechten Ecke des Dialogfelds „Zeichentabelle“ kein Tastenanschlag definiert ist. Weitere Informationen zur Verwendung der Zeichentabelle finden Sie in der Windows Server-Onlinehilfe.

Beispiele für Passwörter, die Zeichen aus dem erweiterten ASCII-Zeichensatz enthalten, sind „kUµ!0o“ und „Wf©$0k#"g¤5ªrd“.

Sie können eine Passwortrichtlinie implementieren, mit der Anforderungen an die Komplexität von Passwörtern erzwungen werden. Weitere Informationen zu dieser Richtlinie finden Sie in der Windows Server-Onlinehilfe unter „Kennwort muss Komplexitätsvoraussetzungen entsprechen“.

Windows-Passwörter können aus bis zu 127 Zeichen bestehen. Wenn sich in einem Netzwerk allerdings auch Computer mit Windows 98 befinden, sollten nur Passwörter mit maximal 14 Zeichen verwendet werden. Microsoft Windows 98 unterstützt bis zu 14 Zeichen. Wenn ein Passwort länger ist, können sich Benutzer möglicherweise nicht über diese Computer am Netzwerk anmelden.

Festlegen der Passwortrichtlinie

Achten Sie beim Festlegen der Passwortrichtlinie darauf, dass für alle Benutzerkonten sichere Passwörter erzwungen werden. Die folgenden Windows Server-Einstellungen erfordern sichere Passwörter.

- Definieren Sie die Richtlinieneinstellung „Kennwortchronik erzwingen“, sodass mehrere frühere Passwörter gespeichert werden. Mit dieser Richtlinieneinstellung können Benutzer ein Passwort nicht noch einmal verwenden, nachdem es abgelaufen ist.

- Definieren Sie die Richtlinieneinstellung „Maximales Kennwortalter“, sodass Passwörter ablaufen, wenn es die Clientumgebung erfordert, üblicherweise alle 30 bis 90 Tage.

- Definieren Sie die Richtlinieneinstellung „Minimales Kennwortalter“, sodass Passwörter erst nach einer bestimmten Anzahl an Tagen geändert werden können. Diese Richtlinieneinstellung funktioniert in Kombination mit der Richtlinieneinstellung „Kennwortchronik erzwingen“. Durch die Festlegung eines minimalen Passwortalters können Benutzer nicht mehrmals ihr Passwort ändern, um die Richtlinieneinstellung „Kennwortchronik erzwingen“ zu umgehen, um anschließend ihr ursprüngliches Passwort verwenden zu können. Benutzer müssen für die angegebene Anzahl an Tagen warten, bis Sie ihr Passwort ändern können.

- Definieren Sie die Richtlinieneinstellung „Minimale Kennwortlänge“, sodass Passwörter mindestens aus der angegebenen Anzahl an Zeichen bestehen müssen. Lange Passwörter – aus sieben oder mehr Zeichen – sind üblicherweise sicherer als kurze. Mit dieser Richtlinieneinstellung können Benutzer keine leeren Passwörter verwenden, und es müssen Passwörter ausgewählt werden, die mindestens aus der angegebenen Anzahl an Zeichen bestehen.

- Aktivieren Sie die Richtlinieneinstellung „Kennwort muss Komplexitätsvoraussetzungen entsprechen“. Mit dieser Richtlinieneinstellung werden alle neuen Passwörter überprüft, um sicherzustellen, dass sie mit den grundlegenden Voraussetzungen für sichere Passwörter übereinstimmen. Eine vollständige Liste dieser Voraussetzungen finden Sie in der Windows Server-Onlinehilfe unter „Kennwort muss Komplexitätsvoraussetzungen entsprechen“.

Definieren einer Kontosperrungsrichtlinie

Gehen Sie beim Definieren einer Kontosperrungsrichtlinie vorsichtig vor. Die Kontosperrungsrichtlinie sollte nicht voreilig eingerichtet werden. Obwohl mit einer Kontosperrungsrichtlinie die Wahrscheinlichkeit erhöht wird, einen nicht autorisierten Angriff auf Ihre Organisation verhindern zu können, besteht die Möglichkeit, dass versehentlich auch autorisierte Benutzer zum Nachteil für Ihre Organisation gesperrt werden.

Wenn Sie sich für eine Kontosperrungsrichtlinie entscheiden, setzen Sie die Richtlinieneinstellung „Kontosperrungsschwelle“ auf einen Wert, der hoch genug ist, sodass Benutzerkonten nicht gleich gesperrt werden, wenn ein autorisierter Benutzer lediglich das Passwort falsch eingegeben hat.

Autorisierte Benutzer können gesperrt werden, wenn sie ihr Passwort auf dem einen Computer ändern, auf einem anderen jedoch nicht. Der Computer, auf dem

das alte Passwort verwendet wird, versucht in diesem Fall kontinuierlich, den Benutzer mit dem alten Passwort zu authentifizieren und sperrt dadurch möglicherweise das Benutzerkonto. Dies kann eine kostspielige Konsequenz aus der Definition einer Kontosperrungsrichtlinie sein, da die autorisierten Benutzer so lange nicht auf Netzwerkressourcen zugreifen können, bis ihre Konten wiederhergestellt sind. Dieses Problem besteht nicht in Organisationen, in denen nur Domänencontroller verwendet werden, die zur Windows Server-Produktfamilie gehören.

Weitere Informationen zur Kontosperrungsrichtlinie finden Sie in der Windows Server-Onlinehilfe unter „Übersicht über die Kontosperrungsrichtlinie". Informationen zur Anwendung bzw. Änderung der Kontosperrungsrichtlinie finden Sie ebenfalls in der Windows Server-Onlinehilfe unter „So wenden Sie eine Kontosperrungsrichtlinie an oder ändern diese".

Zugriffssteuerung

Ein Windows-Netzwerk und die zugehörigen Ressourcen können durch Einbeziehung der Rechte gesichert werden, über die die Benutzer, Gruppen von Benutzern, und Computer im Netzwerk verfügen. Sie können einen oder mehrere Computer sichern, indem Sie Benutzern oder Gruppen bestimmte Benutzerrechte gewähren. Objekte, wie Dateien oder Ordner, können gesichert werden, indem Benutzern oder Gruppen Berechtigungen zugeteilt werden, um ihnen bestimmte Aktionen an diesem Objekt zu gewähren. Die Zugriffssteuerung besteht aus den folgenden Schlüsselkonzepten:

- Berechtigungen
- Objektbesitz
- Vererbung von Berechtigungen
- Benutzerrechte
- Objektüberwachung

Berechtigungen

Durch Berechtigungen wird die Art des Zugriffs festgelegt, die einem Benutzer oder einer Gruppe für ein Objekt oder eine Objekteigenschaft gewährt wird, wie z. B. Dateien, Ordner und Registrierungsobjekte. Berechtigungen werden auf alle gesicherten Objekte angewendet, wie z. B. Dateien oder Registrierungsobjekte. Berechtigungen können allen Benutzern, Gruppen oder Computern gewährt werden. Die Zuteilung von Berechtigungen an Gruppen ist ein bewährtes Verfahren.

Objektbesitz

Bei der Erstellung eines Objekts wird diesem ein Benutzer zugeordnet. In der Standardeinstellung von Windows 2000 Server ist der Ersteller gleichzeitig der Besitzer des Objekts. In Windows Server 2003 wurde dies für Objekte geändert, die von Mitgliedern der Administratorengruppe erstellt werden.

Wenn ein Mitglied der Administratorgruppe in Windows Server 2003 ein Objekt erstellt, wird anstelle des einzelnen Kontos, von dem aus das Objekt erstellt wird, die Administratorengruppe zum Besitzer des Objekts. Dieses Verhalten kann über die lokalen Sicherheitseinstellungen des MMC-Snap-Ins (Microsoft Management Console) mithilfe der Einstellung „Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden". Unabhängig von den Berechtigungen, die für ein Objekt festgelegt sind, kann der Besitzer diese jederzeit

ändern. Weitere Informationen finden Sie in der Windows Server-Onlinehilfe unter „Informationen zum Besitz“.

Vererbung von Berechtigungen

Durch Vererbung können Administratoren Berechtigungen leicht zuweisen und verwalten. Mit dieser Funktion erben Objekte innerhalb eines Containers automatisch alle vererbbaren Berechtigungen dieses Containers. Beispielsweise erben Dateien innerhalb eines Ordners bei deren Erstellung die Berechtigungen für den Ordner. Es werden nur Berechtigungen vererbt, die als vererbbar gekennzeichnet sind.

Benutzerrechte

Benutzerrechte gewähren Benutzern und Gruppen in der Computerumgebung bestimmte Privilegien und Anmelderechte. Informationen zu Benutzerrechten finden Sie in der Windows Server-Onlinehilfe unter „Benutzerrechte“.

Objektüberwachung

Der Zugriff von Benutzern auf Objekte kann überwacht werden. Diese sicherheitsbezogenen Ereignisse können anschließend im Sicherheitsprotokoll der Ereignisanzeige angezeigt werden. Weitere Informationen finden Sie in der Windows Server-Onlinehilfe unter „Überwachung“.

Bewährte Verfahrensweisen der Zugriffssteuerung

Die folgenden Informationen sind relevant, wenn Sie Zugriff auf das Betriebssystem des Servers gewähren bzw. verweigern.

- Weisen Sie Berechtigungen eher Gruppen als Benutzern zu. Da die direkte Wartung einzelner Benutzerkonten ineffizient ist, sollte die Zuweisung von Berechtigungen auf Benutzerbasis eine Ausnahme darstellen.

- Verwenden Sie die Verweigerung von Berechtigungen nur in bestimmten Fällen. Beispielsweise können Sie einen Teil von einer Gruppe von Berechtigungen der gesamten Gruppe ausschließen. Verwenden Sie die Verweigerung von Berechtigungen, wenn Sie einem Benutzer oder einer Gruppe bereits vollen Zugriff gewährt haben.

- Verweigern Sie niemals der Gruppe „Jeder“ den Zugriff auf ein Objekt. Wenn Sie allen die Berechtigung für ein Objekt verweigern, schließt dies die Administratoren mit ein. Eine bessere Lösung ist es, die Gruppe „Jeder“ zu entfernen, solange andere Benutzer, Gruppen oder Objekte über Berechtigungen für dieses Objekt verfügen.

- Weisen Sie Berechtigungen für ein Objekt in der Datenstruktur so hoch wie möglich zu, und wenden Sie dann die Vererbung an, um die Sicherheitseinstellungen in der Struktur zu übertragen. Einstellungen für die Zugriffssteuerung können schnell und effektiv auf alle untergeordneten Objekte oder auf eine Teilstruktur des übergeordneten Objekts angewendet werden. Dadurch erzielen Sie durch minimalen Einsatz den größten Effekt. Die von Ihnen festgelegten Berechtigungseinstellungen sollten für den Großteil der Benutzer, Gruppen und Computer geeignet sein.

- Explizite Berechtigungen können gelegentlich vererbte Berechtigungen überschreiben. Vererbte verweigerte Berechtigungen verhindern den Zugriff auf ein Objekt nicht, wenn das Objekt über einen expliziten Eintrag zur

Erlaubnis verfügt. Explizite Berechtigungen haben Vorrang vor vererbten Berechtigungen. Dies gilt auch für vererbte verweigerte Berechtigungen.

- Bei Active Directory®-Objekten ist es wichtig, die speziellen bewährten Verfahrensweisen für diese Objekte zu verstehen. Weitere Informationen finden Sie in der Windows Server 2003-Onlinehilfe unter „Bewährte Verfahrensweisen für die Zurordnung von Berechtigungen für Active Directory-Objekte“.

Einmaliges Anmelden

Eine Schlüsselfunktion der Authentifizierung in der Windows Server-Produktfamilie ist die Unterstützung der einmaligen Anmeldung. Durch einmaliges Anmelden kann sich ein Benutzer mit einem einzigen Passwort an der Windows-Domäne anmelden und authentifiziert sich somit an allen Computern in der Windows-Domäne, ohne das Passwort erneut eingeben zu müssen.

Einmaliges Anmelden bietet zwei grundlegende Vorteile bezüglich der Sicherheit. Für einen Benutzer ist die Verwendung eines einzelnen Passworts oder einer Smartcard einfacher, wodurch die Arbeitseffizienz erhöht wird. Für Administratoren verringert sich der Supportaufwand für Benutzer der Domäne, da nur ein Konto pro Benutzer verwaltet werden muss.

Die Authentifizierung, einschließlich einmaliger Anmeldung, wird in einem zweiteiligen Vorgang implementiert: Interaktives Anmelden und Netzwerkauthentifizierung. Die erfolgreiche Authentifizierung von Benutzern ist von beiden Elementen abhängig. Weitere Informationen über die Konfiguration der Windows-Funktion zum einmaligen Anmelden finden Sie in der Windows Server-Onlinehilfe.

Externe Sicherheitsfirewall

Bei einer Firewall kann es sich um Hardware oder Software handeln, die verhindert, dass Datenpakete in ein bestimmtes Netzwerk gelangen oder dieses verlassen. Zur Steuerung des Datenverkehrs werden in der Firewall bestimmte nummerierte Ports für Informationspakete geöffnet oder geschlossen. Von der Firewall werden verschiedene Teile der Informationen aller ankommenden und abgehenden Pakete überprüft:

- Das Protokoll, mit dem das Paket gesendet wird
- Das Ziel oder der Absender des Pakets
- Die Art des Inhalts des Pakets
- Die Portnummer, an die es gesendet wird

Wenn die Firewall so konfiguriert ist, dass das angegebene Protokoll am entsprechenden Port akzeptiert wird, kann das Paket passieren. Im Lieferumfang von Microsoft Windows Small Business Server 2003 Premium Edition ist Microsoft Internet Security and Acceleration (ISA) Server 2000 als Firewalllösung enthalten.

ISA Server 2000

Internet Security and Acceleration (ISA) Server 2000 leitet Anfragen und Antworten sicher zwischen Internet und Clientcomputern im internen Netzwerk weiter.

ISA Server dient für Clients im lokalen Netzwerk als sicherer Gateway zum Internet. Der ISA Server-Computer ist für andere Parteien im Kommunikationspfad

transparent. Der Internetbenutzer kann theoretisch nicht erkennen, dass ein Firewallserver vorhanden ist, bis er auf Dienste oder Sites zugreifen möchte, zu denen der Zugriff durch den ISA Server-Computer verweigert wird. Der Internetserver, auf den zugegriffen wird, interpretiert die Anfragen des ISA Server-Computers, als würden diese von der Clientanwendung stammen.

Wenn Sie die IP-Fragmentfilterung (IP – Internet Protocol) auswählen, aktivieren Sie den Webproxy- und Firewall-Dienst für die Filterung von Paketfragmenten. Bei der Filterung von Paketfragmenten werden alle fragmentierten IP-Pakete verworfen. Bei einer häufig verwendeten Angriffsmethode werden fragmentierte Pakete gesendet, die anschließend so zusammengesetzt werden, dass sie dem System schaden können.

ISA Server enthält einen Mechanismus zur Erkennung von Eindringlingen. Im Fall eines Angriffs auf ein Netzwerk wird der Zeitpunkt des Angriffs festgehalten, und eine Reihe konfigurierter Aktionen (oder Warnmeldungen) wird ausgeführt.

Wenn IIS (Internet Information Services, Internetinformationsdienste) auf dem ISA Server-Computer installiert sind, müssen diese so konfiguriert werden, dass nicht die Ports belegt werden, die von ISA Server für ausgehende Webanfragen (standardmäßig 8080) und für eingehende Webanfragen (standardmäßig 80) verwendet werden. Beispielsweise können Sie IIS so ändern, dass Port 81 überwacht wird, und anschließend den ISA Server-Computer so konfigurieren, dass eingehende Webanfragen an Port 81 des lokalen Computers mit IIS geleitet werden.

Wenn ein Konflikt zwischen den von ISA Server und IIS verwendeten Anschlüssen besteht, wird der IIS-Publishingdienst vom Installationsprogramm beendet. Sie können IIS so ändern, dass ein anderer Port überwacht wird, und dann den IIS-Publishingdienst neu starten.

ISA Server-Richtlinien

Sie können eine ISA Server-Richtlinie definieren, durch die der eingehende und ausgehende Zugriff geregelt wird. Durch entsprechende Regeln wird festgelegt, auf welche Sites und Inhalte zugegriffen werden kann. Protokollregeln geben an, ob ein bestimmtes Protokoll für eingehende und ausgehende Kommunikation zugelassen ist.

Es können Regeln für Sites und Inhalte, Protokollregeln, Webpublishingregeln und IP-Paketfilter erstellt werden. Mit diesen Richtlinien wird festgelegt, wie die ISA Server-Clients mit dem Internet kommunizieren und welche Kommunikation zugelassen ist.

Zusätzliche SQL Server 2000-Sicherheitseinstellungen

Da Microsoft Dynamics GP eigentlich auf SQL Server 2000 basiert, ist es wichtig, dass Maßnahmen zur Erhöhung der Sicherheit Ihrer SQL Server 2000-Installation ergriffen werden. Mit den folgenden Schritten kann die Sicherheit von SQL Server verbessert werden:

- Stellen Sie sicher, dass die neuesten Service Packs und Updates der Betriebssysteme und von SQL Server 2000 installiert sind. Informieren Sie sich auf der Microsoft-Website für Sicherheit und Datenschutz (http://www.microsoft.com/security/default.asp, in englischer Sprache) über die neuesten Details.

- Achten Sie für die Sicherheit auf Dateisystemebene darauf, dass alle Daten- und Systemdateien von SQL Server 2000 auf NTFS-Partitionen installiert sind. Die Dateien sollten nur für Benutzer der Administration oder Systemebene mittels NTFS-Berechtigungen zugänglich sein. Dadurch wird der Zugriff von Benutzern auf diese Dateien verhindert, wenn der SQL Server 2000-Dienst (MSSQLSERVER) nicht ausgeführt wird.

- Verwenden Sie für den SQL Server 2000-Dienst (MSSQLSERVER) ein Domänenkonto mit eingeschränkten Rechten oder ein LocalSystem-Konto. Dieses Konto sollte mit minimalen Rechten in der Domäne ausgestattet sein und dabei helfen, einen möglichen Angriff auf den Server einzudämmen, jedoch nicht zu stoppen. Mit anderen Worten sollte dieses Konto nur über Berechtigungen auf lokaler Benutzerebene in der Domäne verfügen. Wenn von SQL Server 2000 ein Domänenadministratorkonto zum Ausführen von Diensten verwendet wird, führt eine Beeinträchtigung des Servers zu einer Beeinträchtigung der gesamten Domäne. Verwenden Sie zum Ändern dieser Einstellung SQL Server Enterprise Manager. Die Zugriffssteuerungslisten (ACL, Access Control List) für Dateien, Registrierung und Benutzerrechte werden automatisch geändert.



Wenn MSDE 2000 mit der Microsoft Dynamics GP-Installation installiert wurde, wird der Dienst in der Standardeinstellung unter dem LocalSystem-Konto ausgeführt.

- Die meisten Versionen von SQL Server 2000 werden mit den zwei Standarddatenbanken „Northwind“ und „Pubs“ installiert. Beide Datenbanken sind Beispieldatenbanken, die zum Testen, Lernen und für allgemeine Beispiele verwendet werden können. Sie sollten nicht in ein Produktionssystem eingebunden werden. Wenn bekannt ist, dass diese Datenbanken verwendet werden, kann ein Angreifer Standardeinstellungen und Standardkonfigurationen ausnutzen. Wenn Northwind und Pubs auf dem SQL Server 2000-Produktionscomputer vorhanden sind, sollten diese entfernt werden. Mit MSDE 2000 werden diese Datenbanken standardmäßig nicht installiert.

- In der Standardeinstellung kann das SQL Server 2000-System nicht überwacht werden, und Zustände werden somit nicht registriert. Dadurch wird die Erkennung von Eindringlingen schwierig, und Angreifer können leichter ihre Spuren verdecken. Zumindest sollte die Überwachung fehlgeschlagener Anmeldeversuche aktiviert sein.

Die aktuellsten Sicherheitsinformationen zu SQL Server 2000 finden Sie unter http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp (in englischer Sprache).

Kapitel 3: Netzwerksicherheit

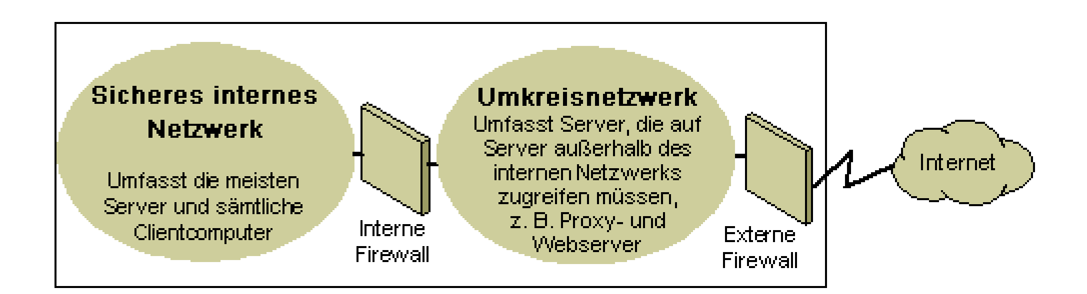
Verwenden Sie die folgenden Informationen, um mehr über die Sicherheit Ihres Netzwerks zu erfahren.

Die Informationen sind in folgende Abschnitte unterteilt:

Strategien für die Netzwerksicherheit

Da Entwurf und Bereitstellung einer IP-Netzwerkumgebung gleichermaßen private wie öffentliche Netzwerkfunktionalität beinhaltet, ist die Firewall zu einer Schlüsselkomponente der Absicherung der Netzwerkintegrität geworden. Eine Firewall ist keine Einzelkomponente. Die NCSA (National Computer Security Association) definiert eine Firewall als „ein System oder eine Kombination von Systemen, die eine Abgrenzung zwischen zwei oder mehr Netzwerken erzwingen". Obwohl verschiedene Begriffe verwendet werden, wird diese Grenze meist als Umkreisnetzwerk bezeichnet. Das Umkreisnetzwerk schützt Ihr Intranet oder Firmen-LAN vor Netzwerkangriffen, indem der Zugriff aus dem Internet oder anderen großen Netzwerken gesteuert wird.

In der folgenden Abbildung ist ein Umkreisnetzwerk dargestellt, das von Firewalls abgegrenzt wird, die sich zwischen einem privaten Netzwerk und dem Internet befinden, um das private Netzwerk zu schützen.



Organisationen verwenden verschiedene Ansätze, um mithilfe von Firewalls für eine Absicherung zu sorgen. Eine IP-Paketfilterung bietet eine schwache Sicherheit, ist mühsam zu verwalten und leicht zu umgehen. Anwendungsgateways sind sicherer als Paketfilter und außerdem leichter zu verwalten, da sie nur einige wenige Anwendungen betreffen, z. B. ein bestimmtes E-Mail-System. Transportschicht-Gateways sind am effektivsten, wenn der Benutzer einer Netzwerkanwendung eine größere Gefährdung darstellt, als die über die Anwendung übertragenen Daten. Der Proxyserver ist ein umfassendes Sicherheitstool, dass einen Anwendungsgateway, sicheren Zugriff für anonyme Benutzer und andere Dienste beinhaltet. Im Folgenden finden Sie weitere Informationen zu den verschiedenen Optionen:

IP-Paketfilterung Die IP-Paketfilterung war die früheste Implementierung der Firewalltechnologie. Paketkopfzeilen werden auf Quell- und Zieladressen, TCP-(Transmission Control Protocol-) und UDP-(User Datagram Protocol-)Anschlussnummern und andere Informationen geprüft. Die Paketfilterung ist eine

eingeschränkte Technologie, die am besten in klaren Sicherheitsumgebungen funktioniert, in denen beispielsweise alle Elementen innerhalb des Umkreisnetzwerks vertrauenswürdig und alle Elemente außerhalb des Umkreisnetzwerks nicht vertrauenswürdig sind. In den letzen Jahren haben verschiedene Anbieter die Paketfilterungsmethode verbessert, indem der Kernpaketfilterung intelligente Entscheidungsfindungsfunktionen hinzugefügt wurden. Dadurch entstand eine neue Form von Firewall mit SPI-Paketfilterung (Stateful Protocol Inspection). Die Paketfilterung kann entweder konfiguriert werden, um (1) bestimmte Pakettypen zuzulassen und alle anderen abzulehnen, oder um (2) bestimmte Pakettypen abzulehnen und alle anderen zuzulassen.

Anwendungsgateways Anwendungsgateways werden verwendet, wenn die Sicherheit des eigentlichen Inhalts einer Anwendung von größter Bedeutung ist. Dass es sich hierbei um eine anwendungsspezifische Methode handelt, hat zugleich Vor- und Nachteile, da eine Anpassung an Technologieänderungen nicht problemlos durchgeführt werden kann.

Transportschicht-Gateways Transportschicht-Gateways sind Tunnel in Firewalls, die bestimmte Vorgänge oder Systeme der einen Seite mit bestimmten Vorgängen oder Systemen auf der anderen Seite verbinden. Transportschicht-Gateways eignen sich am Besten für Umgebungen, in denen der Benutzer einer Anwendung eine größere Gefährdung als die von der Anwendung übertragenen Informationen darstellt. Ein Transportschicht-Gateway unterscheidet sich von einem Paketfilter durch die Möglichkeit, eine Verbindung zu einem Anwendungsschema außerhalb des Bereichs herzustellen, das zusätzliche Informationen hinzufügen kann.

Proxyserver Proxyserver sind umfassende Sicherheitstools, die Firewall- und Anwendungsgatewayfunktionen beinhalten, mit denen der Internetverkehr von und zu einem LAN verwaltet wird. Proxyserver bieten außerdem eine Zwischenspeicherung von Dokumenten und eine Zugriffskontrolle. Ein Proxyserver kann die Leistung verbessern, indem häufig angeforderte Daten zwischengespeichert und direkt bereitgestellt werden (z. B. eine häufig aufgerufeneWebseite). Ein Proxyserver kann Anforderungen außerdem filtern und verwerfen, wenn der Eigentümer diese als nicht geeignet betrachtet, z. B. Anfragen nach nicht autorisiertem Zugriff auf proprietäre Dateien.

Nutzen Sie die Vorteile, die Ihre Organisation aus den Sicherheitsfunktionen einer Firewall gewinnen kann. Positionieren Sie in der Netzwerktopologie ein Umkreisnetzwerk an einer Stelle, an der der gesamte Verkehr von außerhalb des Firmennetzwerks durch den von der externen Firewall verwalteten Umkreis geleitet wird. Die Zugriffssteuerung für die Firewall kann in Übereinstimmung mit den Anforderungen Ihrer Organisation detailliert abgestimmt werden. Außerdem können Firewalls so konfiguriert werden, dass zu sämtlichen nicht autorisierten Zugriffsversuchen ein Bericht erstellt wird.

Um die Anzahl der Anschlüsse zu verringern, die für die innere Firewall geöffnet sein müssen, können Sie eine Firewall auf Anwendungsebene (z. B. ISA Server 2000) verwenden.

Weitere Informationen zu TCP/IP finden Sie in „Designing a TCP/IP Network“ unter http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp (in englischer Sprache).

Drahtlose Netzwerke

In der Standardeinstellung werden drahtlose Netzwerke in der Regel so konfiguriert, dass ein Abhören der drahtlosen Datenübertragung möglich ist. Sie sind durch die Standardeinstellungen einiger drahtloser Hardware, die Zugriffsmöglichkeiten sowie aktuelle Verschlüsselungsmethoden anfällig für unerwünschten externen Zugriff. Das Abhören kann mithilfe einiger Konfigurationsoptionen und Tools verhindert werden. Beachten Sie jedoch, dass die Computer damit nicht vor Hackern und Viren geschützt sind, die über die Internetverbindung eindringen. Daher ist es äußerst wichtig, eine Firewall zu verwenden, die die Computer vor unerwünschtem Eindringen über das Internet schützt.

Weitere Informationen zum Schutz eines drahtlosen Netzwerks finden Sie in „Wie Sie die Sicherheit Ihres drahtlosen 802.11b-Heimnetzwerks erhöhen“ unter:

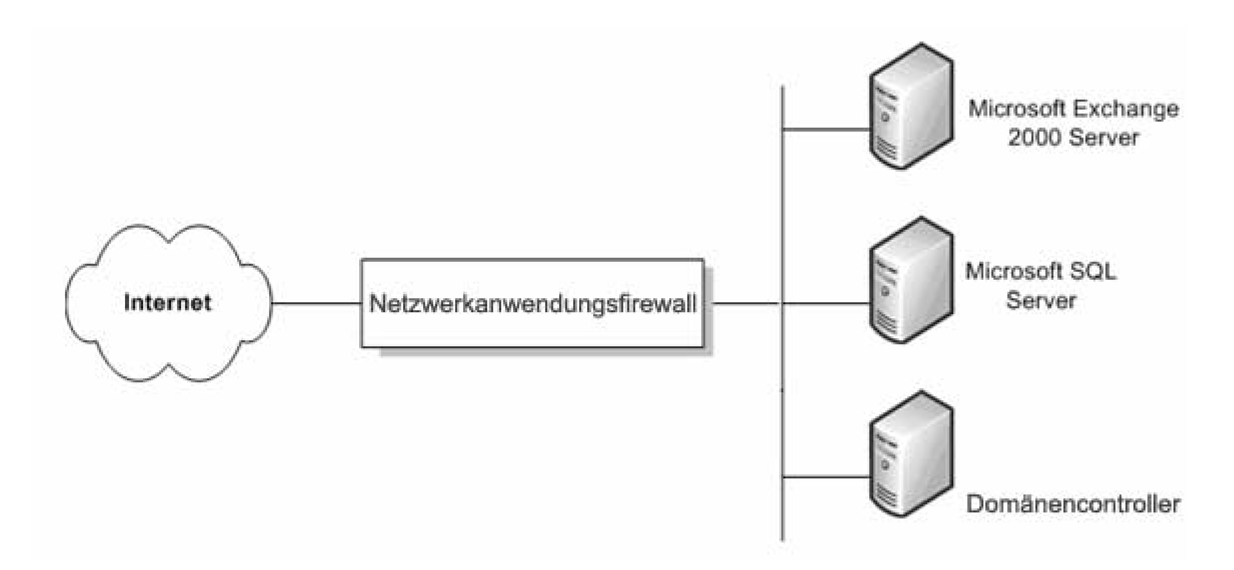
http://support.microsoft.com/default.aspx?scid=kb;en-de;309369.

Netzwerksicherheitsszenarios

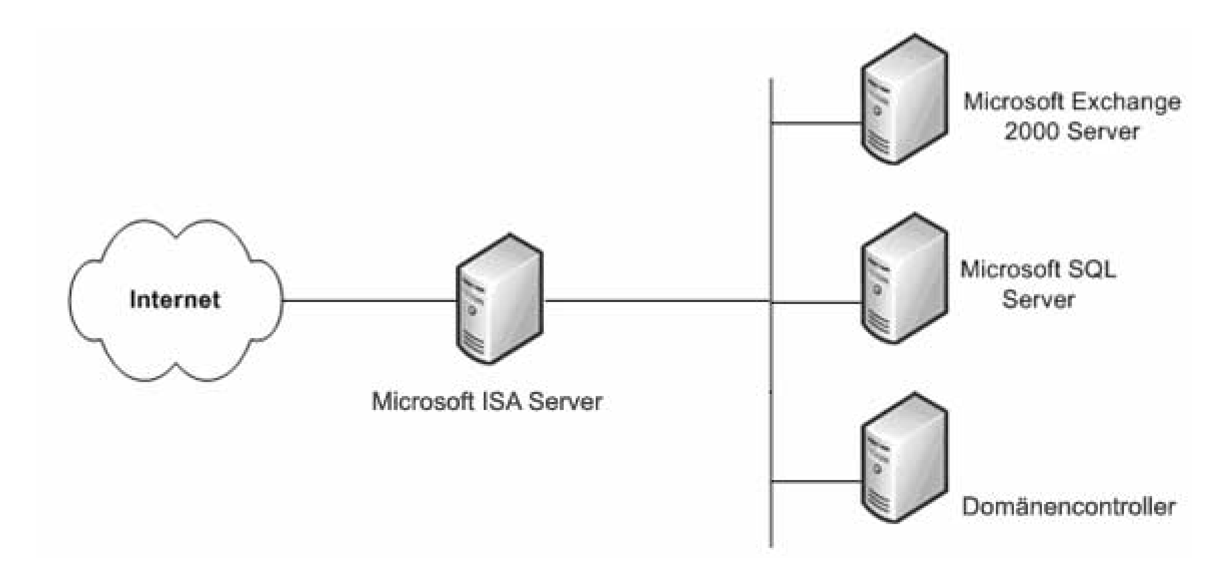
Die für Ihre Organisation erforderliche Netzwerksicherheitsstufe hängt von unterschiedlichen Faktoren ab. In der Regel läuft es auf einen Kompromiss zwischen dem Budget und der Notwendigkeit hinaus, die Firmendaten zu schützen. Für ein kleines Unternehmen ist es möglich, eine äußerst komplexe Sicherheitsstruktur bereitzustellen, die für das Netzwerk die höchstmögliche Sicherheitsstufe bietet. Diese Sicherheitsstufe ist jedoch für kleinere Unternehmen häufig nicht finanzierbar. In diesem Abschnitt werden vier Szenarios erläutert. Außerdem finden Sie jeweils entsprechende Empfehlungen für verschiedene Sicherheitsstufen zu angemessen Kosten.

Keine Firewall Wenn Ihre Organisation über eine Internetverbindung, jedoch nicht über eine Firewall verfügt, müssen einige Maßnahmen zur Netzwerksicherheit implementiert werden. Es gibt einfache Netzwerkfirewallanwendungen, die ausreichend Sicherheit bieten, um die meisten möglichen Hackerangriffe zu verhindern (siehe nächster Abschnitt).

Eine einfache Firewall Die minimal empfohlene Sicherheitsstufe ist eine einfache Firewall zwischen dem Internet und Ihren Daten. Diese Firewall bietet möglicherweise keine erweiterte Sicherheitsstufe und sollte nicht als sehr sicher betrachtet werden. Sie ist jedoch besser als kein Schutz.



Hoffentlich gestattet Ihr Budget eine sicherere Lösung für den Schutz Ihrer Firmendaten. Eine solche Lösung stellt ISA Server dar. Die höheren Kosten dieses zusätzlichen Servers bieten wesentlich größere Sicherheit als eine herkömmliche Firewall, da diese in der Regel lediglich eine Netzwerkadressübersetzung (NAT) und Paketfilterung enthält.

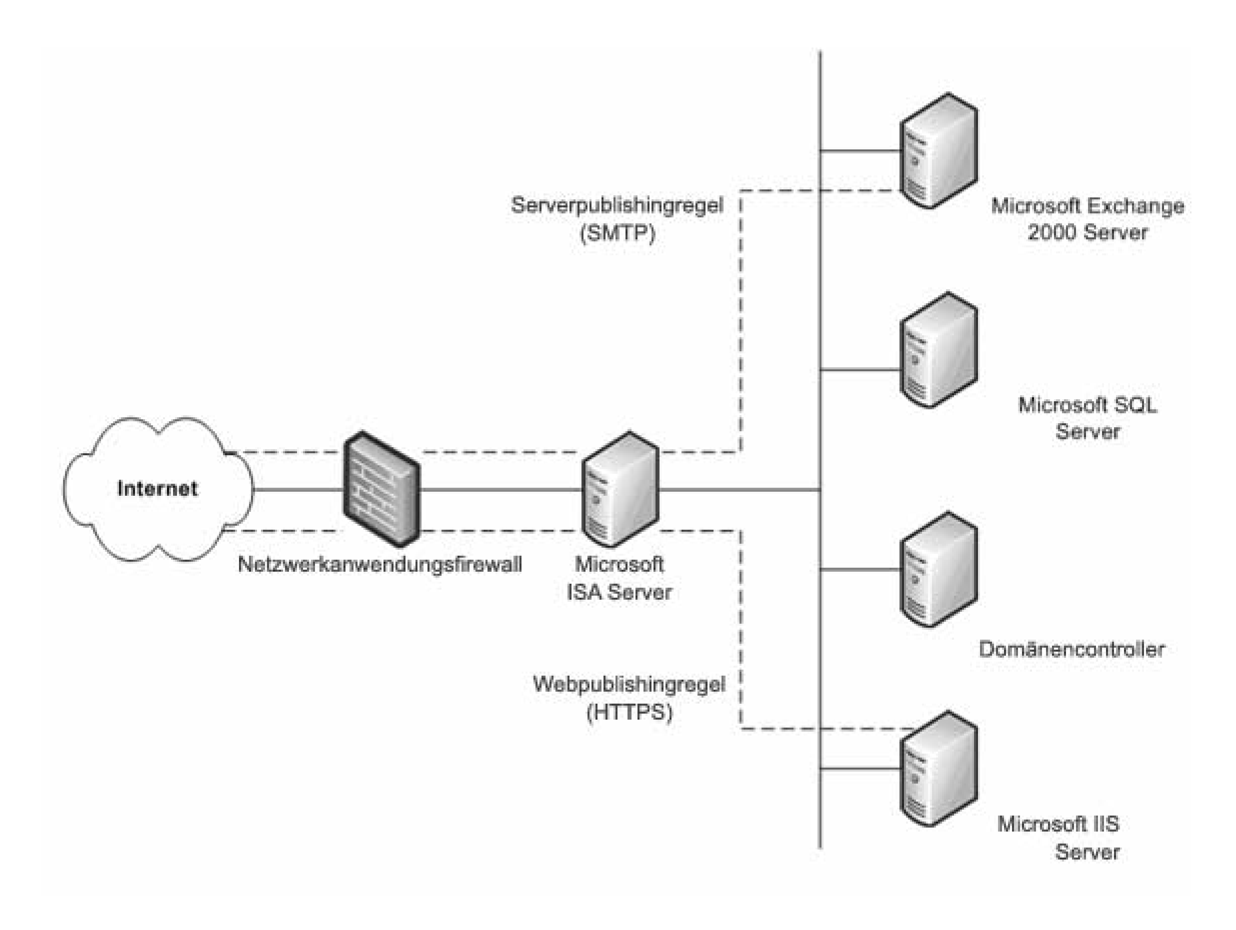


Diese Lösung mit einer einzelnen Firewall ist sicherer als eine Firewallanwendung der Einstiegsstufe und bietet Windows-spezifische Sicherheitsdienste.

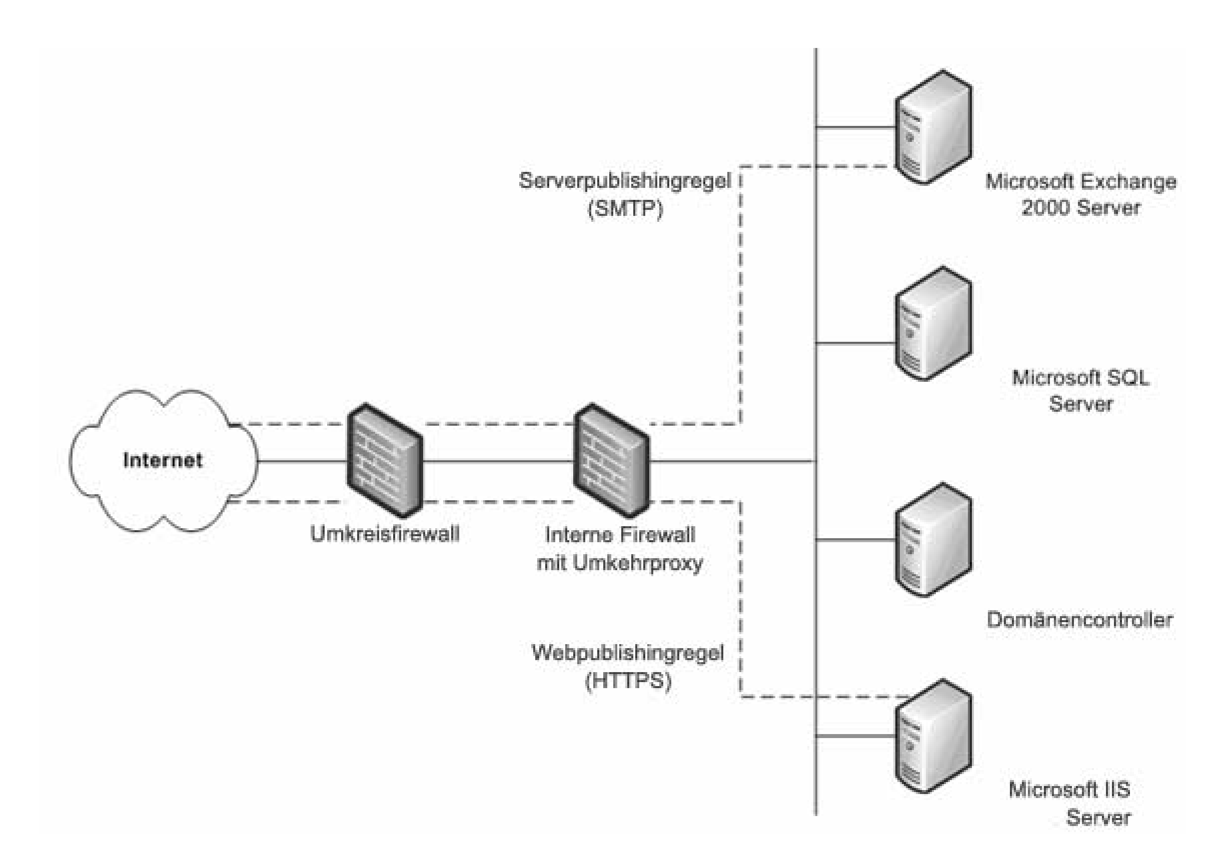
Eine vorhandene Firewall Wenn bereits eine Firewall vorhanden ist, die Ihr Intranet vom Internet trennt, kann eine zusätzliche Firewall in Betracht gezogen werden, die mehrere Methoden für das Konfigurieren der internen Ressourcen für das Internet ermöglicht.

Eine solche Methode ist Webpublishing. Hierbei wird ein ISA Server vor dem Webserver des Unternehmens bereitgestellt, der den Internetzugriff für die Benutzer ermöglicht. Bei eingehenden Webanfragen kann ISA Server für die Außenwelt einen Webserver verkörpern, der Clientanfragen auf Webinhalte über den Cache ausführt. ISA Server leitet Anfragen nur dann an den Webserver weiter, wenn diese Anfragen nicht über den Cache beantwortet werden können.

Eine weitere Methode ist Serverpublishing. ISA Server ermöglicht das Veröffentlichen interner Server im Internet, ohne die Sicherheit des internen Netzwerks zu gefährden. Sie können Regeln zum Web- und Serverpublishing konfigurieren, die festlegen, welche Anfragen an einen Server im lokalen Netzwerk gesendet werden sollen, sodass den internen Servern eine weitere Sicherheitsstufe hinzugefügt wird.



Zwei vorhandene Firewalls Das vierte Szenario beinhaltet zwei in einem bestehenden Umkreisnetzwerk implementierte Firewalls (DMZ). Mindestens einer dieser Server bietet umgekehrte Proxydienste, sodass Internetclients nicht direkt auf Intranetserver zugreifen. Stattdessen fängt eine der beiden Firewalls (im Idealfall die interne) die Netzwerkanfragen an interne Server ab, überprüft die Pakete und leitet sie anschließend im Auftrag des Internethosts weiter.



Dieses Szenario ähnelt dem vorherigen, nachdem die zweite Firewall hinzugefügt wurde. Der einzige Unterschied besteht darin, dass die interne Firewall, die umgekehrte Proxydienste unterstützt, kein ISA Server ist. In diesem Szenario sollten Sie eng mit den für die jeweiligen Firewalls Verantwortlichen zusammenarbeiten, um Serverpublishingregeln zu definieren, die die Sicherheitsrichtlinie einhalten.

Kapitel 4: Virenschutz

Verwenden Sie die folgenden Informationen, um mehr über die verschiedenen Typen von Computerviren und die Möglichkeiten, Ihr Unternehmen vor der Infektion mit einem Computervirus zu schützen, zu erfahren.

Die Informationen sind in folgende Abschnitte unterteilt:

- *Übersicht über Viren*
- *Virentypen*

Übersicht über Viren

Ein Computervirus ist eine ausführbare Datei, die entwickelt wurde, um sich selbst zu replizieren, Datendateien und Programme zu beschädigen oder zu löschen und um einer Erkennung zu entgehen. Viren werden häufig neu geschrieben und angepasst, sodass sie nicht erkannt werden können. Viren werden häufig als E-Mail-Anhänge gesendet. Antivirenprogramme müssen regelmäßig aktualisiert werden, um nach neuen und geänderten Viren zu suchen. Viren sind die häufigste Methode der Computerkriminalität.

Antivirensoftware wurde entwickelt, um Virenprogramme zu erkennen und zu verhindern. Da ständig neue Virenprogramme entwickelt werden, bieten viele Anbieter von Antivirenprodukten regelmäßige Aktualisierungen ihrer Software an. Microsoft empfiehlt dringend, in Ihrer Organisationsumgebung Antivirensoftware zu implementieren.

Virensoftware wird in der Regel an einem der drei folgenden Orte installiert: den Benutzerarbeitsstationen, den Servern und dem Netzwerk der Organisation, an dem E-Mails eingehen (und in einigen Fällen ausgehen).

Weitere Informationen zu Viren und Computersicherheit im Allgemeinen finden Sie auf den folgenden Microsoft-Sicherheitswebsites:

- Microsoft Sicherheits-Portal (http://www.microsoft.com/germany/sicherheit/default.mspx).

- Sicherheitsdokumentation in Microsoft TechNet (http://www.microsoft.com/germany/technet/sicherheit/Default.mspx).

Virentypen

Folgende vier Haupttypen von Viren infizieren Computersysteme: Startsektorviren, Viren, die Dateien infizieren, trojanische Pferde und Makroviren.

Startsektorviren Beim Starten des Computers wird vor dem Laden des Betriebssystems oder anderer Startdateien der Startsektor der Festplatte durchsucht. Startsektorviren ersetzen die Informationen im Startsektor der Festplatte durch eigenen Code. Wenn ein Computer mit einem Starsektorvirus infiziert ist, wird vor allen anderen Elementen der Virencode in den Speicher geladen. Wenn sich der Virus im Speicher befindet, kann er sich auf sämtliche anderen verwendeten Festplatten auf dem infizierten Computer verbreiten.

Viren, die Dateien infizieren Hierbei handelt es sich um den am häufigsten auftretenden Virentyp. Er hängt sich selbst an eine ausführbare Programmdatei,

indem er dieser seinen eigenen Code hinzufügt. Der Virencode wird in der Regel so hinzugefügt, dass er einer Erkennung entgeht. Wenn die infizierte Datei ausgeführt wird, kann sich der Virus an andere ausführbare Dateien anhängen. Die von diesem Virentyp infizierten Dateien verfügen normalerweise über eine der Dateierweiterungen COM, EXE oder SYS.

Einige dieser Viren wurden für bestimmte Programme entwickelt. Häufig wird auf Programmtypen wie OVL-(Overlay) und DLL-(Dynamic Link Library) Dateien abgezielt. Diese Dateien werde zwar nicht ausgeführt, jedoch von ausführbaren Dateien aufgerufen. Der Virus wird beim Aufruf übertragen.

Der Schaden an den Daten tritt auf, wenn der Virus ausgelöst wird. Ein Virus kann ausgelöst werden, indem eine infizierte Datei ausgeführt oder eine bestimmte Umgebungseinstellung (z. B. ein bestimmtes Systemdatum) eintritt.

Trojanische Pferde Bei einem trojanischen Pferd handelt es sich nicht um einen wirklichen Virus. Der Hauptunterschied zwischen einem Virus und einem trojanischen Pferd besteht darin, dass sich ein trojanisches Pferd nicht selbst repliziert, es zerstört lediglich Informationen auf der Festplatte. Ein trojanisches Pferd gibt sich selbst als legitimes Programm aus, z. B. als Spiel oder Dienstprogramm. Wenn es ausgeführt wird, kann es Daten zerstören oder beschädigen.

Makroviren Bei einem Makrovirus handelt es sich um einen Computervirentyp, der in einem Makro innerhalb einer Datei, einer Vorlage oder einem Add-In gespeichert wird. Die Ausbreitung eines Makrovirus kann verhindert werden. Folgende Tipps zum Vermeiden einer Infektion sollten Sie in Ihrer Organisation bekannt machen.

- Installieren Sie eine Virenschutzlösung, die eingehende Meldungen aus dem Internet auf Viren durchsucht, bevor diese den Router passieren. Dadurch wird sichergestellt, dass E-Mails auf bekannte Viren durchsucht werden.
- Die Quelle der empfangenen Dokumente sollte bekannt sein. Dokumente sollten nur geöffnet werden, wenn der Benutzer den Absender für vertrauenswürdig hält.
- Sprechen Sie mit der Person, die das Dokument erstellt hat. Wenn Benutzer nicht genau wissen, ob ein Dokument sicher ist, sollten sie sich an den Ersteller wenden.
- Verwenden Sie den Microsoft Office-Makrovirenschutz. In Office werden die Benutzer gewarnt, wenn ein Dokument Makros enthält. Diese Funktion ermöglicht es Benutzern, die Makros beim Öffnen des Dokuments zu aktivieren oder zu deaktivieren.
- Verwenden Sie Virensuchsoftware, um Makroviren zu erkennen und zu entfernen. Virensuchsoftware kann Makroviren in Dokumenten erkennen und entfernen. Microsoft empfiehlt die Verwendung von Antivirensoftware, die von der ICSA (International Computer Security Association) zertifiziert ist.

- Setzen Sie die Makrosicherheitsstufe von Microsoft Office-Dateien auf „Hoch“ oder „Mittel“, und verwenden Sie digitale Signaturen. Eine digitale Signatur ist ein elektronischer, verschlüsselungsbasierter sicherer Stempel zur Authentifizierung eines Makros oder Dokuments. Die Signatur bestätigt, dass das Makro oder Dokument vom Signaturgeber stammt und nicht geändert wurde. Weitere Informationen zu Microsoft Office-Sicherheitsfeatures finden Sie auf der Microsoft Office Online-Website (http://office.microsoft.com/de-de/default.aspx).

Kapitel 5: Microsoft Dynamics GP Sicherheit

Microsoft Dynamics GP bietet mehrere Arten von Sicherheit. Im Folgenden erhalten Sie eine Übersicht über die Sicherheitsfeatures in Microsoft Dynamics GP.

Schrittweise Anleitungen zum Einrichten der Sicherheit in der Microsoft Dynamics GP-Anwendung finden Sie in Teil 2, „Benutzer Setup" und Teil 5, „Unternehmensstruktur" der Microsoft Dynamics GP System Setup-Dokumentation.

Informationen zur Verwendung der erweiterten Sicherheit finden Sie im Handbuch zur erweiterten Sicherheit von Microsoft Dynamics GP.

Beide Handbücher sind über die Option „Druckbare Handbücher" im Menü „Hilfe" von Microsoft Dynamics GP verfügbar oder können auf der CustomerSource-Website heruntergeladen werden.

Zur effektiveren Verwaltung von Berechtigungen verwendet Microsoft Dynamics GP feste Rollen und Datenbankrollen von Microsoft SQL Server.

Die Informationen sind in folgende Abschnitte unterteilt:

Bereiche, die von Sicherheitseinstellungen betroffen sind

Die folgenden Bereiche von Microsoft Dynamics GP sind von Sicherheitseinstellungen betroffen.

System Die Systemberechtigungen steuern den Zugriff auf systemweite Setupinformationen, wie z. B. das Erstellen neuer Firmen, das Einrichten neuer Benutzerdatensätze, das Zuordnen von Benutzerberechtigungen oder das Drucken von Berichten mit diesen Informationen. Die Berechtigungen auf Systemebene werden durch die Verwendung eines Passworts gesteuert.

Firma Firmenberechtigungen steuern für jeden einzelnen Benutzer den Zugriff auf Firmen. Wenn ein Administrator einen neuen Benutzerdatensatz einrichtet, hat die betreffende Person keinen Zugriff auf Firmen. Dem neuen Benutzer muss über das Fenster „Benutzerzugriff Setup" Zugriff gewährt werden, bevor dieser sich bei Microsoft Dynamics GP anmelden kann.



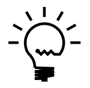
Wenn ein neuer Benutzer hinzugefügt wird, hat dieser in der Standardeinstellung Zugriff auf fast alle Informationen der Firma, bis dieser Zugriff eingeschränkt wird.

Fenster Wenn einem Benutzer in Microsoft Dynamics GP der Zugriff auf eine Firma gewährt wird, kann dieser in der Standardeinstellung auf fast alle Fenster des Systems zugreifen. Ein Systemadministrator kann den Zugriff auf Fenster innerhalb des Systems benutzerspezifisch steuern, entweder explizit oder durch die Verwendung von Benutzerklassen.

Bericht Wenn einem Benutzer in Microsoft Dynamics GP der Zugriff auf eine Firma gewährt wird, kann dieser in der Standardeinstellung auf alle Berichte im System zugreifen. Ein Systemadministrator kann den Zugriff auf Berichte innerhalb des Systems benutzerspezifisch steuern, entweder explizit oder durch die Verwendung von Benutzerklassen. Wenn ein Bericht geändert oder erstellt wird, haben Benutzer in der Standardeinstellung jedoch keinen Zugriff auf diesen Bericht. Der Zugriff muss gewährt werden, bevor Benutzer den neuen bzw. geänderten Bericht anzeigen können.

Tabellen Wenn einem Benutzer in Microsoft Dynamics GP der Zugriff auf eine Firma gewährt wird, kann dieser in der Standardeinstellung auf alle Tabellen im System zugreifen. Ein Systemadministrator kann den Zugriff auf Tabellen innerhalb des Systems benutzerspezifisch steuern, entweder explizit oder durch die Verwendung von Benutzerklassen. Durch das Verweigern des Zugriffs auf eine Tabelle in Microsoft Dynamics GP kann der entsprechende Benutzer keine Berichte ausdrucken, die diese Tabelle verwenden. Der Benutzer kann jedoch weiterhin Fenster öffnen und Prozesse ausführen, für die ein Zugriff auf diese Tabelle erforderlich ist.

Modulspezifische Aufgaben Die meisten Module von Microsoft Dynamics GP haben bestimmte Aufgaben, die so eingerichtet werden können, dass ein Passwort erforderlich ist. Jede Aufgabe kann über ein eigenes Passwort verfügen. Wenn ein Passwort erforderlich ist, muss jeder Benutzer zum Ausführen dieser Aufgabe zuerst das Passwort eingeben. In der Dokumentation für die Systemeinrichtung finden Sie Informationen zu diesen Passwörtern für jedes einzelne Buchhaltungsmodul.



Wenn Sie mehrere Firmen in Microsoft Dynamics GP einrichten (und die erweiterte Sicherheit von Microsoft Dynamics GP nicht verwenden), beziehen sich die Berechtigungsoptionen für einzelne Benutzer nur auf eine Firma, während sich die Berechtigungsoptionen für Benutzerklassen auf alle Firmen beziehen. Bei Verwendung der erweiterten Sicherheit von Microsoft Dynamics GP können Sie Berechtigungsänderungen mehreren Firmen zuordnen.

Gewähren einer Zugriffsberechtigung

Ein Systemadministrator kann den Zugriff von einzelnen Benutzern oder Gruppen von Benutzern (Benutzerklassen) auf Teile des Microsoft Dynamics GP-Systems in allen Firmen verweigern. Klassen werden über das Fenster „Benutzerklassen Setup“ erstellt, und einzelne Benutzer werden den Klassen über das Fenster „Benutzer Setup“ zugeordnet.

Wenn Sie zum Ändern von Berichten Report Writer oder Modifier verwenden, muss ein Administrator individuelle Berechtigungen einrichten oder Benutzerklassen verwenden, um Zugriff auf geänderte Berichte und Fenster zu gewähren. Die Artikeltypen, die durch Benutzerklassen oder individuelle Berechtigungen gesteuert werden können, sind später unter *Artikel, für die Berechtigungen eingestellt werden können* auf Seite 32 aufgeführt.

Es ist zu empfehlen, dass alle Mitglieder einer Klasse innerhalb von Microsoft Dynamics GP über dieselben Zugriffsberechtigungen verfügen. Wenn einer gesamten Klasse Zugriffsrechte gewährt oder verweigert werden und die Änderungen auf jeden in dieser Klasse übertragen werden, entsprechen die Zugriffsberechtigungen der einzelnen Mitglieder den der Klasse zugeordneten Zugriffsberechtigungen . Wenn Änderungen an den Zugriffsberechtigungen für einzelne Mitglieder der Klasse vorgenommen wurden, werden diese Änderungen von Zugriffsberechtigungen überschrieben, die der gesamten Klasse zugewiesen werden. Wenn alle Benutzer über leicht unterschiedliche Zugriffsberechtigungen verfügen sollen oder ein Benutzer Zugriff auf verschiedene Teile von Microsoft Dynamics GP innerhalb verschiedener Firmen haben soll, erstellen Sie für jeden Zugriffstyp eine separate Klasse.

Eine weitere Möglichkeit zum Gewähren ähnlicher Zugriffstypen für verschiedene Benutzer ist die Verwendung der Funktion „Kopieren“ der erweiterten Sicherheit. Mit der Funktion „Kopieren“ können die Zugriffsberechtigungen eines Benutzers auf andere Benutzer übertragen werden oder die Zugriffsberechtigungen eines Benutzers für eine Firma auf zusätzliche Firmen ausgeweitet werden. Die neue Zugriffsberechtigung kann geändert werden, wenn der Benutzer einen leicht abgeänderten Zugriff benötigt.

Einzelne Benutzer Neben den Berechtigungen der Benutzerklasse oder anstelle dieser Berechtigungen bieten individuelle Zugriffsberechtigungen Flexibilität beim Anpassen der Berechtigungseinstellungen für einzelne Benutzer. Ein Administrator kann den Zugriff auf Teile des Microsoft Dynamics GP-Systems für einzelne Benutzer und Firmen im Fenster „Berechtigungen einrichten“ gewähren oder verweigern.

Modulspezifische Aufgaben Die meisten Module von Microsoft Dynamics GP haben bestimmte Aufgaben, die so eingerichtet werden können, dass ein Passwort erforderlich ist. Jede Aufgabe kann über ein eigenes Passwort verfügen. Wenn ein Passwort erforderlich ist, muss jeder Benutzer zum Ausführen dieser Aufgabe zuerst das Passwort eingeben. In der Dokumentation für die Systemeinrichtung finden Sie Informationen zu diesen Passwörtern für jedes einzelne Buchhaltungsmodul.

Informationen zur Verwendung von Passwörtern in Microsoft Dynamics GP

Microsoft Dynamics GP steuert mithilfe von Passwörtern den Zugriff auf eine Firma und ausgewählte Teile des Buchhaltungssystems. Passwörter können Großbuchstaben, Kleinbuchstaben, numerische Zeichen, Satzzeichen und Leerstellen enthalten. Es gibt drei Typen von Passwörtern.

Benutzerpasswörter Benutzerpasswörter steuern den Zugriff bestimmter Benutzer auf Microsoft Dynamics GP. Benutzerpasswörter werden anfänglich im Fenster „Benutzer Setup“ von einem Administrator festgelegt oder beim ursprünglichen Installationsvorgang von Microsoft Dynamics GP eingegeben. Die Benutzer können ihr eigenes Passwort im Fenster „Benutzerpasswort Setup“ ändern.

Systempasswörter Das Systempasswort steuert den Zugriff auf systemweite Setupinformationen, wie z. B. das Einrichten neuer Benutzerdatensätze, das Zuordnen von Benutzerberechtigungen oder das Drucken von Berichten mit diesen Informationen. Das Systempasswort wird im Fenster „Systempasswort einrichten“ geändert.

Aufgabenpasswörter Die meisten Module von Microsoft Dynamics GP haben bestimmte Aufgaben, die so eingerichtet werden können, dass ein Passwort erforderlich ist. Jede Aufgabe kann über ein eigenes Passwort verfügen. Wenn ein Passwort erforderlich ist, muss jeder Benutzer zum Ausführen dieser Aufgabe zuerst das Passwort eingeben. In der Dokumentation für die Systemeinrichtung finden Sie Informationen zu diesen Passwörtern für jedes einzelne Buchhaltungsmodul.

Artikel, für die Berechtigungen eingestellt werden können

Über das Fenster „Benutzerklassen Setup" können Sie auf Microsoft Dynamics GP-Artikel für eine Benutzerklasse zugreifen. Den Zugriff für einen einzelnen Benutzer und eine einzelne Firma richten Sie im Fenster „Berechtigungen einrichten" ein.

Für die folgenden Artikel in Microsoft Dynamics GP und integrierte Produkte können Sie Berechtigungen festlegen.

Artikel	Beschreibung
Fenster	Fenster im ausgewählten Produkt
Berichte	Berichte im ausgewählten Produkt
Geänderte Fenster	Fenster, die mit Modifier angepasst wurden
Geänderte Berichte	Primärkopien von Berichten, die mit Report Writer erstellt wurden Hinweis: In der Liste wird der Report Writer-Name des Berichts angezeigt. Dabei handelt es sich um den Namen, der beim Drucken eines Berichts in der Titelleiste des Fensters „Bildschirmausgabe" angezeigt wird.
Dateien	Tabellen im ausgewählten Produkt
Alternative Microsoft Dynamics GP-Berichte*	Microsoft Dynamics GP-Berichte, die in von Ihnen installierte integrierte Produkte aufgenommen wurden
Alternative Microsoft Dynamics GP-Fenster*	Microsoft Dynamics GP-Fenster, die in von Ihnen installierte integrierte Produkte aufgenommen wurden
Geänderte alternative Microsoft Dynamics GP-Berichte*	Alternative Berichte, die mit Report Writer geändert wurden
Geänderte alternative Microsoft Dynamics GP-Fenster*	Alternative Fenster, die mit Modifier geändert wurden
Kundenberichte	Sekundärkopien und neue Berichte, die in Report Writer erstellt wurden
Erweiterte Finanzberichte	Geänderte erweiterte Finanzberichte
Modulbuchungsgenehmigungen	Bestimmte Buchungsaufgaben für jedes Microsoft Dynamics GP-Produkt, das Sie erworben haben
Individuelle Tools	Hilfsprogramme wie Report Writer oder Modifier, die Sie verwenden, um das Buchhaltungssystem anzupassen. Neue Benutzer haben in der Standardeinstellung keinen Zugriff darauf. Ihnen muss der Zugriff erst gewährt werden.
Microsoft Dynamics GP-Import **	Microsoft Dynamics GP-Integrationsmanager. Hiermit werden zusätzlich Berechtigungen für das Import-Utility mit Microsoft Dynamics GP festgelegt. Neue Benutzer haben in der Standardeinstellung keinen Zugriff darauf. Ihnen muss der Zugriff erst gewährt werden.
Dokumentenzugriff	Angebote, Bestellungen, Rechnungen, Retouren und Nachlieferungen für die Vertriebsverarbeitung. Standard- and Direktlieferungsbestellungen für die Bestellungsverarbeitung.
*Diese Artikel werden nur angezeigt, wenn Sie ein integriertes Produkt verwenden und es in der Produktliste ausgewählt haben. **Diese Typen werden nur angezeigt, wenn der entsprechende Artikel installiert und registriert ist.	

Erweiterte Sicherheit

Die erweiterte Sicherheit bietet Benutzern eine alternative Benutzeroberfläche zum Einrichten von Berechtigungen in Microsoft Dynamics GP. Außerdem können Sie die Berechtigungseinstellungen von Klassen zuordnen, ohne dass dies Auswirkungen auf andere Änderungen an Ressourcen auf Benutzerebene hat. Die Oberfläche enthält eine Funktion zum Einrichten derselben Berechtigungseinstellungen für mehrere Benutzer, Klassen oder Firmen.

Die erweiterte Sicherheit enthält die folgenden Funktionen:

- Eine grafische Oberfläche für einfache Bedienung.
- Berechtigungseinstellungen für Klassen, die übertragen werden können, ohne dass dies Auswirkungen auf andere Änderungen an Ressourcen auf Benutzerebene hat.
- Eine Kopierfunktion, mit der die Zugriffsberechtigungen eines Benutzers auf andere Benutzer übertragen werden können oder die Zugriffsberechtigungen eines Benutzers für eine Firma auf zusätzliche Firmen ausgeweitet werden können.
- Berechtigungen für SmartLists sind in die erweiterte Sicherheit integriert, sodass diese nicht in einem separaten Fenster eingerichtet werden müssen.
- Die Möglichkeit, die Ansicht zu wechseln (nach Wörterbuch oder nach Navigationsmenü) beim Einrichten von Berechtigungen.
- Die Möglichkeit, Änderungen zu speichern, bis die Einrichtung von Berechtigungen abgeschlossen ist, und diese anschließend zu einem beliebigen Zeitpunkt auf das System anzuwenden.

Weitere Informationen finden Sie im Handbuch zur erweiterten Sicherheit von Microsoft Dynamics GP.



Wenn Sie die erweiterte Sicherheit verwenden möchten, um die Berechtigungen für Ihre Firma einzurichten und zu verwalten, sollten alle Berechtigungen mit der erweiterten Sicherheit festgelegt werden, anstatt einige Optionen dort festzulegen und andere in den ursprünglichen Berechtigungsfenstern von Microsoft Dynamics GP.

Sicherheit auf Feldebene

Die Sicherheit auf Feldebene bietet zusätzliche Sicherheit für Felder in Microsoft Dynamics GP. Im Fenster „Sicherheit auf Feldebene“ werden alle Benutzer, Benutzerklassen und Firmen angezeigt, die mit der erweiterten Sicherheit erstellt oder geändert wurden. Gleichzeitig gelten alle Änderungen an Benutzern und Klassen, die im Fenster „Sicherheit auf Feldebene“ vorgenommen werden, auch für die erweiterte Sicherheit. Im Fenster „Sicherheit auf Feldebene“ können Sie Passwörter zuordnen und Felder, Formulare und Fenster ausblenden oder deaktivieren.

Anwendungssicherheit

Die folgenden Informationen helfen Ihnen, zu verstehen, wie Anwendungssicherheit in Microsoft Dynamics GP verwaltet wird.

- Zu den Aufgaben, die von einem Administrator durchgeführt werden müssen, zählt das Erstellen von Sicherheitskopien, Firmen und neuen Benutzer IDs.

- Der Datenbankbesitzer wird für alle Microsoft Dynamics GP-Datenbanken auf DYNSA gesetzt. Es ist wichtig, dass DYNSA als Besitzer aller Microsoft Dynamics GP-Datenbanken erhalten bleibt. Wenn ein anderer Besitzer zugewiesen wird, können beim Löschen von Benutzerkonten und beim Erteilen von Zugriffsberechtigungen für Firmen Komplikationen auftreten.

- Alle Benutzer müssen über gültige Passwörter verfügen, um sich an der Anwendung anzumelden. Wird ein leeres Passwort erkannt, wird der Benutzer aufgefordert, das Passwort vor dem Anmelden an der Anwendung zu ändern. Außerdem wird empfohlen, alle inaktiven Benutzerkonten zu löschen oder ihnen ein gültiges Passwort zuzuweisen und sie von allen Firmenzugriffen auszuschließen.

- In der Standardeinstellung hat kein Benutzerkonto in Microsoft Dynamics GP Zugriff auf die Fenster „Individualisierungsverwaltung", „Individualisierungsstatus", „Microsoft Dynamics GP Import" sowie auf Modifier, Report Writer, Personalabteilungsbriefe und auf die System-Mastertabelle.

- Beispielbenutzer haben lediglich Zugriff auf die Beispielfirma.

- Die Verwendung der festen Server- und Datenbankrollen von Microsoft SQL Server wurde erweitert, sodass Benutzer, die diesen Rollen zugewiesen sind, nun Zugriff auf die Funktionen in Microsoft Dynamics GP haben, wofür früher ein Benutzerkonto mit dem Status des Systemadministrators („sa") erforderlich war.

Microsoft Dynamics GP Utilities-Sicherheit

Alle Mitglieder der festen Serverrolle „SysAdmin" können ein Upgrade einer vorherigen Version durchführen oder Microsoft Dynamics GP installieren.

Sicherheit für neue Installationen

Microsoft Dynamics GP Utilities überprüft, ob die DYNSA-Anmeldung vorhanden ist. Wenn diese nicht existiert, wird die Anmeldung erstellt, und der Benutzer muss ein Passwort eingeben, um fortzufahren. DYNSA ist für ALLE Microsoft Dynamics GP-Datenbanken als Datenbankbesitzer eingestellt.

- Beim Erstellen der DYNSA-Anmeldung wird diese den festen Serverrollen „SecurityAdmin" und „dbCreator" zugewiesen.

- Jeder Benutzer mit den entsprechenden SQL-Berechtigungen kann Microsoft Dynamics GP installieren.

- Beim Installieren der Beispielfirma müssen Passwörter angegeben werden, wenn die BEISPIELBENUTZER-Konten erstellt werden.

- Wenn die Anmeldungen DYNSA, LESSONUSER1 und LESSONUSER2 erstellt werden, haben diese keinen Zugriff auf die Tabelle „SY02400" (Tabelle „System - Passwort-Master"). Mit diesen Anmeldungen ist somit kein Zugriff über Report Writer auf diese Tabelle möglich.

Upgrade einer früheren Version

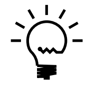
- Wenn sich der Systemadministrator („sa“) an Microsoft Dynamics GP Utilities anmeldet, wird von der Anwendung überprüft, ob das Passwort für DYNSA entweder <leer> oder „ZUGRIFF“ ist. In beiden Fällen muss der Benutzer ein neues DYNSA-Passwort eingeben, um mit dem Upgrade fortzufahren.

- Der Zugriff auf die Tabelle „SY02400“ (Tabelle „System - Passwort-Master“) in Report Writer wird für alle Benutzer entfernt.

- Beim Erstellen der DYNSA-Anmeldung wird diese automatisch den festen Serverrollen „SecurityAdmin“ und „dbCreator“ zugewiesen.

Office-Smarttags

Microsoft Office-Smarttag Manager wird zum Einrichten und Aktivieren von Office-Smarttags in der Microsoft Dynamics GP-Anwendung verwendet. Microsoft Office-Smarttags sind nicht an Microsoft Dynamics GP-Berechtigungen gebunden.



Office-Smarttag-Manager kann separat auf der CustomerSource-Website im Bereich „Downloads & Updates“ heruntergeladen werden. Ausführliche Anweisungen zum Installieren von Office-Smarttags finden Sie im Handbuch zu Microsoft Dynamics GP Office-Smarttags.

Office-Smarttags basieren auf Netzwerkgruppen, sodass Benutzer mit allgemeinen Geschäftsanforderungen (wie z. B. Kundendienstmitarbeiter, Geschäftsanalysten oder Vertriebsmitarbeiter) auf den gleichen Satz Smarttags und die gleichen Firmendatenbanken zugreifen können. Die Netzwerkgruppen sollten vor der Installation von Office-Smarttag-Manager geplant und eingerichtet werden. Nach der Installation von Office-Smarttag-Manager und der Erstellung der Netzwerkgruppen mit Benutzern, die den entsprechenden Gruppen hinzugefügt wurden, muss der Zugriff der einzelnen Netzwerkgruppen auf die jeweiligen Einträge, Aktionen und Firmen im Office-Smarttag-Manager festgelegt werden.

Die Verfügbarkeit von Einträgen und Aktionen kann einzeln oder gleichzeitig festgelegt werden. Wenn ein Eintrag nicht verfügbar ist, sind auch alle zugehörigen Aktionen nicht verfügbar.

Bevor Office-Smarttag-Manager für die Mitglieder einer Gruppe verfügbar ist, müssen Sie dieser Gruppe auf mindestens einen Eintrag, eine Aktion und eine Firma Zugriff gewähren.

Office-Smarttags werden durch den Typ der Daten oder des Eintrags gekennzeichnet, den sie von Microsoft Dynamics-Anwendungen anerkennen. Von jedem Eintrag können verschiedene Aktionen durchgeführt werden. Die Aktionen enthalten direkte Verbindungen zu den Microsoft Dynamics-Anwendungen von Office.

Für jede Office-Smarttag-Manager-Gruppe muss der Zugriff auf die Smarttag-Einträge gewährt werden, die den Geschäftsanforderungen der Gruppe entsprechen. Beispielsweise kann für Kundendienstmitarbeiter der Zugriff auf die Smarttags „Kunde“, „Artikel“ und „Konto“ und für Geschäftsanalysten der Zugriff auf alle Microsoft-Smarttags wichtig sein. Außerdem muss der Zugriff auf Aktionen für alle aktivierten Smarttag-Einträge entsprechend den Anforderungen der Gruppe gewährt werden. Beispielsweise können für Kundendienstmitarbeiter, deren einzige Aufgabe die Beantwortung von Kundenbestellanfragen ist, nur

Aktionen für das Anzeigen aktiviert werden, anstelle ihnen den Zugriff auf Anwendungsfenster zu gewähren.

Für jede Office-Smarttag-Manager-Gruppe muss außerdem der Zugriff auf bestimmte Firmen innerhalb einer Microsoft Dynamics-Anwendung gewährt werden. Dieser Zugriff sollte sich an den allgemeinen Geschäftsanforderungen der Benutzer orientieren.



Wenn ein Benutzer Mitglied in mehreren Office-Smarttag-Manager-Gruppen ist, verfügt dieser Benutzer nur über Zugriff auf Smarttag-Einträge, Aktionen und Firmen, die in allen Gruppen aktiviert sind. Wenn ein Eintrag, eine Gruppe oder eine Firma in einer der Gruppen nicht verfügbar ist, kann der Benutzer nicht darauf zugreifen. Außerdem können Sie einer Netzwerkgruppe nicht den Namen „SmartTags" geben, da diese Zeichenfolge ein reservierter Name in der Anwendung ist.

Problembehandlung bei Berechtigungen

Bei vielen Vorgängen in Microsoft Dynamics GP, etwa beim Buchen und Drucken, ist es erforderlich, dass der den Vorgang durchführende Benutzer Zugriff auf mehrere Fenster, Berichte und Tabellen hat. Wenn ein Benutzer keinen Zugriff auf einen Artikel hat, der Teil des Vorgangs ist, kann der Vorgang nicht abgeschlossen werden. Gegebenenfalls wird eine Meldung mit dem Hinweis angezeigt, dass der Benutzer nicht berechtigt ist, die Ressource zu öffnen. Es wird jedoch nicht in allen Fällen eine Meldung mit einem Hinweis auf das Problem angezeigt. Wenn der Zugriff auf Tabellen verweigert wurde, kann dadurch lediglich nicht auf Berichte zugegriffen werden, die auf die jeweilige Tabelle zugreifen.

Wenn Sie die erweiterte Sicherheit verwenden, können Sie im zugehörigen Fenster die Berechtigungseinstellungen für Benutzerdatensätze sowie die mit den Benutzern verknüpften Firmen oder Klassen überprüfen, um sicherzustellen, dass keine Fehler vorliegen. Für mögliche Fehler gibt es die Option, den Fehler zu beheben, alle erkannten Fehler zu beheben oder keine Fehler zu beheben.

Kapitel 6: Das Microsoft Dynamics GP-Datenbanksicherheitsmodell

Verwenden Sie diese Informationen, um mehr über das Microsoft Dynamics GP-Datenbanksicherheitsmodell zu erfahren.

Diese Informationen sind in folgende Abschnitte unterteilt:

Passwortsicherheit

Benutzerkonten müssen innerhalb der Microsoft Dynamics GP-Anwendung erstellt werden. So wird gewährleistet, dass die Sicherheit auf alle Microsoft Dynamics GP-Fenster und -Berichte angewendet wird. In Microsoft Dynamics GP wird das Passwort während des Benutzererstellungsprozesses vor der Übergabe an Microsoft SQL Server verschlüsselt. Wenn beispielsweise ein Benutzerkonto mit dem Passwort „1234“ vor dem Erstellen des Benutzerkontos in Microsoft SQL Server erstellt wird, durchläuft dieses Passwort den Microsoft Dynamics GP-Verschlüsselungsprozess und wird beispielsweise in „ABCD“ geändert. So können lediglich die Microsoft Dynamics GP-Anwendung sowie weitere Anwendungen, die den Microsoft Dynamics GP-Verschlüsselungsprozess verwenden, das Benutzerpasswort vor dem Senden an Microsoft SQL Server übersetzen.

Wenn ein Benutzer versucht, von außerhalb der Microsoft Dynamics GP-Anwendung auf Microsoft SQL Server zuzugreifen, wird der Anmeldeversuch abgelehnt, da dia Passwörter nicht übereinstimmen. Um diesen Vorgang noch sicherer zu machen, können Benutzer in Microsoft Dynamics GP das Passwort nicht in leer oder unverschlüsselt ändern.

Die Datenbankrolle „DYNGRP“

Für das Sichern von Daten müssen ausführliche Kenntnisse über die Datenbankrolle „DYNGRP“ vorhanden sein. Die Datenbankrolle „DYNGRP“ wird für den Zugriff auf in der Datenbank vorhandene Objekte wie Tabellen, gespeicherte Prozeduren und Ansichten verwendet. Dadurch wird das Zuweisen bestimmter Berechtigungen zu Datenbankobjekten erleichtert. Wenn der Datenbank „DYNGRP“ die Berechtigungen „SELECT“, „UPDATE“, „INSERT“, „DELETE“ und „EXECUTE“ für alle Objekte in der Datenbank gewährt werden, muss einzelnen Benutzern nicht über SQL-DBAs und die Microsoft Dynamics GP-Anwendung ausdrücklich Zugriff gewährt werden. Stattdessen sind die einzelnen Microsoft Dynamics GP-Benutzer Mitglieder der Datenbank „DYNGRP“ und erben somit dieselben Berechtigungen. Wenn ein Administrator einem Benutzer Zugriff auf eine Firma in Microsoft Dynamics GP gewährt, wird dieser auch ein Mitglied von „DYNGRP“ der entsprechenden Datenbank.

Da diese Datenbankrolle zusammen mit der Microsoft Dynamics GP-Anwendung verwendet wird, ist es wichtig zu wissen, dass ausschließlich Microsoft Dynamics GP-Benutzer Mitglieder dieser Rolle sein sollten. Wenn Benutzerkonten ohne verschlüsselte Passwörter innerhalb dieser Datenbankrolle platziert werden, haben diese Benutzer möglicherweise über andere Anwendungen Zugriff. Wenn andere Anwendungen Zugriff auf Microsoft Dynamics GP-Daten benötigen, sollte der Administrator neue Datenbankrollen mit Berechtigungen erstellen, die lediglich

für die Objekte gelten, auf die einzelne Benutzer zugreifen müssen. Mithilfe dieser Vorgehensweisen kann das Risiko verringert werden, dass nicht autorisierte Benutzer auf Ihre Daten zugreifen können.

Hinzufügen eines Benutzerkontos zur festen Serverrolle „SysAdmin"

Es gibt zwei Typen von SQL Server-Rollen: fester Server und Datenbank. Feste Serverrollen werden verwendet, um SQL Server zu verwalten und Funktionen durchzuführen, die die Verfügbarkeit von SQL Server und von Prozessen betreffen, z. B. das Erstellen von Datenbanken und das Hinzufügen von Anmeldungen. Datenbankrollen werden verwendet, um die Datenbank zu verwalten, der die Datenbankrolle zugewiesen ist. Zu den Datenbankverwaltungsfunktionen gehört das Gewähren von Benutzerzugriff, das Gewähren von Berechtigungen für Datenbankobjekte und das Sichern der Datenbank selbst. Der Prozess für das Hinzufügen eines Benutzers zu einer festen Serverrolle oder zu einer Datenbankrolle ist identisch.

So fügen Sie ein Benutzerkonto zur festen Serverrolle „SysAdmin" hinzu

1. Stellen Sie sicher, dass die SQL-Anmeldung in Microsoft SQL Server vorhanden ist. Öffnen Sie Enterprise Manager, und klicken Sie auf das „+" neben dem SQL Server-Namen und anschließend auf das „+" neben dem Sicherheitsordner. Klicken Sie anschließend auf das Anmeldesymbol, um die Anmeldungen im rechten Fensterbereich anzuzeigen. Wenn die gesuchte Anmeldung nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf das Anmeldesymbol, und wählen Sie die Option „Aktualisieren" aus, um Ihre Anmeldung anzuzeigen.

2. Zeigen Sie die Liste der festen Serverrollen an. Klicken Sie auf die das Symbol für die Serverrollen, um im rechten Fensterbereich eine Liste sämtlicher fester Serverrollen anzuzeigen.

3. Fügen Sie die Anmeldung der festen Serverrolle hinzu. Doppelklicken Sie auf das Systemadministratorsymbol im rechten Fensterbereich, um die „SysAdmin"-Informationen der Serverrolleneigenschaften anzuzeigen. Klicken Sie auf die Schaltfläche „Hinzufügen", und wählen Sie die Anmeldung aus, der die Rolle hinzugefügt werden soll.

Wenn Sie diese Schritte durchgeführt haben, wird die Anmeldung erfolgreich der festen Serverrolle „SysAdmin" hinzugefügt, und die Anmeldung erbt sofort die entsprechenden Berechtigungen. Für jede Datenbank sind Datenbankrollen vorhanden. Befolgen Sie dieselben Schritte, um einen Benutzer zu einer Datenbankrolle hinzuzufügen.

Kapitel 7: Sicherheitsaufgaben für Hauptanwendungen

Im Folgenden finden Sie Informationen zu den häufigsten Sicherheitsaufgaben der Hauptanwendungen sowie einige Optionen für die Durchführung dieser Aufgaben. Diese Optionen verfügen über verschiedene Sicherheitsstufen. Die Option mit der höchsten Nummer entspricht der jeweils sichersten Option für die einzelnen Aufgaben.

Die Informationen sind in folgende Abschnitte unterteilt:

Erstellen von Benutzerdatensätzen

Das Erstellen und Verwalten von Benutzerkonten in Microsoft Dynamics GP gehört zu den wichtigsten Aufgaben, da es das Gewähren von Zugriff auf Daten beinhaltet. SQL Server-Datenbankadministratoren können Microsoft Dynamics GP-Benutzern eine minimale Anzahl an Berechtigungen gewähren, die erforderlich ist, um basierend auf den Einstellungen im Fenster „SQL Optionen“ in der Microsoft Dynamics GP-Anwendung Anmeldungen und Benutzerkonten zu erstellen. Die folgenden Optionen stehen zur Verfügung. Die sicherste Auswahl ist Option 5.

Optionen

1. Melden Sie sich bei Microsoft Dynamics GP als Systemadministrator („sa“) an, und erstellen Sie die erforderlichen Benutzer (keine Änderungen zu früheren Versionen). Bei Microsoft Dynamics GP-Administratorkonten kann es ich um beliebige Benutzerkonten innerhalb der Anwendung handeln.

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten der festen Serverrolle „SysAdmin“ zu. Der aktuelle Benutzer muss in der Datenbank „DYNAMICS“ ein Mitglied von „DYNGRP“ sein, um gespeicherte Prozeduren durchführen zu können. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln.

3. Weisen Sie die Besitzeranmeldung „DYNSA“ der DYNAMICS-Datenbank zur festen Serverrolle „SecurityAdmin“ zu, und melden Sie sich mit dem Benutzer „DYNSA“ beim Client an.

4. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten der festen Serverrolle „SysAdmin“ zu. Dies gilt auch für die Datenbankrolle „Db_Owner“, die sich in der DYNAMICS-Datenbank befindet. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln. Bei „DYNSA“ muss es sich jedoch um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

5. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten der festen Serverrolle „SysAdmin“ zu. Dies gilt auch für die Datenbankrollen „Db_AccessAdmin“ und „Db_SecurityAdmin“, die in der DYNAMICS-Datenbank vorhanden sind. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln. Bei „DYNSA“ muss es sich jedoch um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

Löschen von Benutzerdatensätzen

Das Löschen von Benutzerdatensätzen ist für die Sicherheit ebenso wichtig, wie das Erstellen von Benutzerkonten. Daher stehen für das Löschen der Benutzerdatensätze dieselben Optionen wie für das Erstellen zur Verfügung. Die folgenden Optionen stehen zur Verfügung: Die sicherste Auswahl ist Option 5.

Optionen

1. Melden Sie sich bei der Anwendung als Systemadministrator („sa“) an, und löschen Sie die erforderlichen Benutzerdatensätze (keine Änderungen zu früheren Versionen).

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten zur festen Serverrolle „SysAdmin“ zu. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln.

3. Weisen Sie die Datenbankbesitzeranmeldung „DYNSA“ der festen Serverrolle „SecurityAdmin“ zu, und melden Sie sich unter „DYNSA“ beim Client an. Bei dieser Option muss es sich bei „DYNSA“ um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

4. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten der festen Serverrolle „SysAdmin“ zu. Dies gilt auch für die Datenbankrolle „Db_Owner“, die in allen Microsoft Dynamics GP-Datenbanken vorhanden ist. Beim Microsoft Dynamics GP-Administrator kann es sich um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln.

5. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten der festen Serverrolle „SysAdmin“ zu. Dies gilt für die Datenbankrolle „Db_AccessAdmin“, die in allen Microsoft Dynamics GP-Datenbanken vorhanden ist. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln. Bei „DYNSA“ muss es sich jedoch um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

Gewähren von Benutzerzugriff

Die für das Gewähren des Zugriffs auf eine Firmendatenbank erforderlichen Schritte in Microsoft Dynamics GP Version 9.0 entsprechen denen früherer Versionen. Der Benutzer muss jedoch über ausreichende Berechtigung für das Gewähren des Zugriffs auf eine Firmendatenbank verfügen. Die folgenden Optionen stehen zur Verfügung: Die sicherste Auswahl ist Option 5.

Optionen

1. Melden Sie sich bei der Anwendung als Systemadministrator („sa“) an, und gewähren Sie den erforderlichen Zugriff (keine Änderungen zu früheren Versionen).

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten zur festen Serverrolle „SysAdmin“ zu. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln.

3. Melden Sie sich als Datenbankbesitzer an („DYNSA“). Bei dieser Option muss es sich bei „DYNSA“ um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

4. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten zur Datenbankrolle „Db_Owner Database“ zu, die in allen Microsoft Dynamics GP-Datenbanken vorhanden ist. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln. Bei „DYNSA“ muss es sich jedoch um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

5. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten den Datenbankrollen „Db_AccessAdmin“ und „Db_SecurityAdmin“ zu, die in allen Microsoft Dynamics GP-Datenbanken vorhanden sind. Dank dieser Option kann es sich beim Microsoft Dynamics GP-Administrator um ein beliebiges Benutzerkonto innerhalb der Microsoft Dynamics GP-Anwendung handeln. Bei „DYNSA“ muss es sich jedoch um den Datenbankbesitzer ALLER Microsoft Dynamics GP-Datenbanken handeln.

Sichern von Datenbanken

Die folgenden Optionen stehen zur Verfügung. Die sicherste Auswahl ist Option 4.

Optionen

1. Melden Sie sich bei der Anwendung als Systemadministrator („sa“) an, und führen Sie die erforderliche Sicherung durch (keine Änderungen zu früheren Versionen).

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten zur festen Serverrolle „SysAdmin“ zu.

3. Melden Sie sich bei der Anwendung mit der Datenbankbesitzeranmeldung („DYNSA“) an.

4. Weisen Sie die jeweiligen Microsoft Dynamics GP-Benutzer-SQL-Anmeldekonten der Datenbankrolle „Db_BackupOperator“ zu. Da sich Microsoft Dynamics GP-Administratoren bei dieser Option nicht als SQL Server-Systemadministrator anmelden müssen, handelt es sich hierbei um die sicherste Option.

Wiederherstellen von Datenbanken

In der Microsoft Dynamics GP-Anwendung gibt es eine Option für das Wiederherstellen von Datenbanken. Da die Gefahr besteht, dass diese Funktion missbraucht wird, um Daten zu ändern, zu entfernen oder zu beschädigen, beschränkt sich der Zugriff auf das Fenster „Firma wiederherstellen“ auf die Systemadministratorenanmeldung („sa“).

Firmenwarnungen

Das Erstellen und Ausführen von Firmenwarnungen beinhaltet einige Funktionen und erfordert einige Zugriffsrechte in Microsoft SQL Server. Firmanwarnungen erstellen gespeicherte Prozeduren und Microsoft SQL Server-Aufträge. Außerdem können E-Mail-Nachrichten an Benutzer gesendet werden. Daher müssen die entsprechenden Berechtigungen nicht nur für die Firmendatenbanken, sondern auch für Objekte gewährt werden, die sich in den Master- und MSDB-Datenbanken befinden. Beim Erstellen dieser Objekte muss auch die Objekteigentümerschaft bedacht werden. Dies gilt insbesondere für Microsoft SQL Server-Aufträge. Daher wurde die Option für das Erstellen von Firmenwarnungen auf zwei begrenzt. Die sicherste Auswahl ist Option 2.

Optionen

1. Melden Sie sich bei der Anwendung als Systemadministrator („sa“) an, und erstellen Sie die erforderliche Firmenwarnung (keine Änderungen zu früheren Versionen).

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten zur festen Serverrolle „SysAdmin“ zu. Da sich Microsoft Dynamics GP-Administratoren bei dieser Option nicht als SQL Server-Systemadministrator anmelden müssen, handelt es sich hierbei um die sicherste Option.

SQL-Verwaltung

Das Fenster „SQL Verwaltung“ bietet die Möglichkeit, Tabellen und gespeicherte Prozeduren in der Microsoft Dynamics GP-Anwendung zu erstellen oder zu verwerfen. Der Systemadministrator („sa“) und der Datenbankbesitzer („DYNSA“) verfügen über Zugriff auf dieses Fenster. Dieser Zugriff kann auch anderen Anmeldungen zugewiesen werden. Es gibt drei Möglichkeiten, Zugriff auf dieses Fenster zu erhalten. Die sicherste Auswahl ist Option 3.

Optionen

1. Melden Sie sich bei der Anwendung als Systemadministrator („sa“) an, um auf das Fenster zuzugreifen (keine Änderungen zu früheren Versionen).

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten der festen Serverrolle „SysAdmin“ zu, und greifen Sie mit diesem Konto auf das Fenster zu.

3. Melden Sie sich als Datenbankbesitzer („DYNSA“) an, um auf das Fenster zuzugreifen. Da sich Microsoft Dynamics GP-Administratoren bei dieser Option nicht als SQL Server-Systemadministrator anmelden müssen, handelt es sich hierbei um die sicherste Option.

Löschen von Firmen

Das Fenster „Firma löschen“ wird verwendet, um Microsoft Dynamics GP-Firmen zu löschen. Die folgenden Optionen stehen zur Verfügung: Option 3 ist die sicherste Option.

Optionen

1. Melden Sie sich bei der Anwendung als Systemadministrator („sa“) an, und führen Sie die entsprechenden Schritte durch (keine Änderungen zu früheren Versionen).

2. Weisen Sie die jeweiligen Microsoft Dynamics GP-Administrator-SQL-Anmeldekonten zur festen Serverrolle „SysAdmin“ zu.

3. Melden Sie sich als Datenbankbesitzer an („DYNSA“). Da sich Microsoft Dynamics GP-Administratoren bei dieser Option nicht als SQL Server-Systemadministrator anmelden müssen, handelt es sich hierbei um die sicherste Option.

Löschen verwaister Benutzerkonten

Benutzer können ihre eigenen verwaisten Konten ohne den Eingriff eines Administrators löschen. Gegebenenfalls kann diese Option über eine Microsoft Dexterity®- oder VISUAL BASIC® FOR APPLICATIONS-Änderung entfernt werden.

Kapitel 8: Häufig gestellte Fragen

In den folgenden Informationen sind häufig gestellte Fragen in Bezug auf Microsoft Dynamics GP enthalten.

Die Informationen sind in folgende Abschnitte unterteilt:

- *Benutzerkonten*
- *Microsoft Dynamics GP-Fenster*
- *Sicherheit in Microsoft Dynamics GP*

Benutzerkonten

Nachfolgend finden Sie Antworten auf Fragen zu Benutzerkonten.

Warum ist für ein Benutzerkonto der Zugriff auf alle Microsoft Dynamics GP-Datenbanken erforderlich, um ein anderes Benutzerkonto zu löschen?

Beim Löschen eines Benutzerkontos wird die SQL-Anmeldung gelöscht, und das Benutzerkonto wird von Microsoft Dynamics GP aus allen Datenbanken entfernt, in denen es Mitglied ist. Der aktuelle Benutzer benötigt Zugriff auf alle Datenbanken sowie die enstsprechenden Berechtigungen zum Löschen des Benutzerkontos aus SQL Server. Wenn der aktuelle Benutzer keinen Zugriff auf die Datenbank hat, um ein Benutzerkonto zu entfernen, wird eine entsprechende Warnmeldung angezeigt.

Muss sich das Benutzerkonto bei allen Datenbanken in derselben Datenbankrolle befinden?

Technisch gesehen muss der Benutzer nicht bei allen Datenbanken derselben Datenbankrolle angehören. Es wird jedoch dringend empfohlen. Es ist möglich, dass ein Benutzer in einer Datenbank der Rolle DB_OWNER angehört und in einer anderen den Rollen DB_ACCESSADMIN und DB_SECURITYADMIN. Je nach Festlegung besteht dann weiterhin die Möglichkeit, Benutzern Zugriff auf Firmendatenbanken zu gewähren. Alle Benutzer von Microsoft Dynamics GP sollten jedoch der Datenbankrolle DYNGRP angehören, damit die Anwendung einwandfrei funktioniert.

Microsoft Dynamics GP-Fenster

Nachfolgend finden Sie Antworten auf Fragen zu den Fenstern in Microsoft Dynamics GP.

Warum sind beim Öffnen des Fensters „Benutzerzugriff“ die Kontrollkästchen nicht verfügbar?

Wenn die Voraussetzungen zur Verwendung des Fensters „Benutzerzugriff“ nicht erfüllt werden, sind die Kontrollkästchen nicht verfügbar. Im Fenster „Benutzerzugriff“ besteht die Möglichkeit, den Zugriff auf Unternehmen zu gewähren oder zu verweigern. Dieser Vorgang zum Gewähren und Verweigern des Zugriffs umfasst lediglich das Hinzufügen und Entfernen von Benutzerkonten in der Datenbank sowie die Zuteilung des Benutzers zur Rolle DYNGRP. Ob die Kontrollkästchen verfügbar sind, ist von den folgenden beiden Faktoren abhängig:

- Die Datenbankberechtigungen des aktuellen Benutzers, wenn das Fenster geöffnet wird.
- Der Benutzer, von dem der Vorgang durchgeführt wird, verfügt über die entsprechenden Berechtigungen, die im Abschnitt zum Benutzerzugriff in diesem Dokument erläutert werden. Es besteht keine Möglichkeit, die Verfügbarkeit von Kontrollkästchen aufgrund der im Datenbankfenster festgelegten Berechtigungen einzeln zu deaktivieren.

Warum ist die Schaltfläche „Speichern" im Fenster „Benutzer Setup" nicht verfügbar?

Die Schaltfläche „Speichern" ist deaktiviert, wenn der aktuelle Benutzer nicht über die entsprechenden Berechtigungen zum Erstellen eines Benutzerkontos verfügt. Wenn der aktuelle Benutzer nicht der festen Serverrolle „SysAdmin" angehört, muss eine Kombination aus SQL Server-Rollen verwendet werden, um die Anmeldung zu erstellen. Der aktuelle Benutzer muss ein Mitglied der festen Serverrolle „SysAdmin" sein und mindestens ein Mitglied der Rolle „Db_Owner" oder der Rollen „Db_AccessAdmin" und „Db_SecurityAdmin" für die DYNAMICS-Datenbank.

Warum ist die Schaltfläche „Löschen" im Fenster „Benutzer Setup" nicht verfügbar?

Die Schaltfläche „Löschen" ist deaktiviert, wenn der aktuelle Benutzer nicht über die entsprechenden Berechtigungen zum Löschen eines Benutzerkontos verfügt. Wenn der aktuelle Benutzer nicht der festen Serverrolle „SysAdmin" angehört, muss eine Kombination aus SQL Server-Rollen verwendet werden, um die Anmeldung zu erstellen. Der aktuelle Benutzer muss ein Mitglied der festen Serverrolle „SecurityAdmin" sein und mindestens ein Mitglied der Rolle „Db_Owner" oder „Db_AccessAdmin" für alle in der Tabelle „Firma – Master" (SY01500) enthaltenen Datenbanken. Wenn in der Tabelle „Firma – Master" Datensätze ohne eine zugehörige Datenbank enthalten sind, müssen diese entfernt werden, damit die Schaltfläche „Löschen" verfügbar wird.

Warum ist die Feld „Passwort" im Fenster „Benutzer Setup" nicht verfügbar?

Das Feld „Passwort" ist nicht verfügbar, wenn die Benutzer-ID des Systemadministrators („sa") in das Fenster „Benutzer Setup" eingegeben wird. Das „sa"-Benutzerpasswort kann innerhalb der Microsoft Dynamics GP-Anwendung nicht geändert werden, da es durch die Verwendung und Verschlüsselung in anderen Microsoft SQL Server-Tools unbrauchbar wäre.

Warum sind einige der Passwortfelder („Benutzer muss das Kennwort bei der nächsten Anmeldung ändern", „Kennwortrichtlinie erzwingen" und „Ablauf des Kennwortes erzwingen") im Fenster „Benutzer Setup" nicht verfügbar, und wie kann ich diese Felder verwenden?

Diese Funktionen werden nur unterstützt, wenn Microsoft Dynamics GP zusammen mit Microsoft SQL Server 2005 und Windows Server 2003 verwendet wird. Bei der Verwendung mit Microsoft SQL Server 7.0 oder Microsoft SQL Server 2000 werden diese Funktionen nicht unterstützt.

Sicherheit in Microsoft Dynamics GP

Nachfolgend finden Sie Antworten auf Fragen zur Sicherheit in Microsoft Dynamics GP.

Werden SQL Server-Rollen von der Microsoft Dynamics GP-Anwendung erkannt?

Die folgenden Microsoft SQL Server-Rollen werden von Microsoft Dynamics GP erkannt und verwendet. Andere Rollen werden nicht überprüft, um Zugriff auf Funktionen in Microsoft Dynamics GP zu gewähren oder zu verweigern. Es ist erforderlich, dass jeder Benutzer von Microsoft Dynamics GP ein Mitglied der Datenbankrolle „DYNGRP" für alle Microsoft Dynamics GP-Datenbanken ist.

- Feste Serverrolle „SysAdmin" – Alle Vorgänge in SQL Server können durchgeführt werden. Die Berechtigungen dieser Rolle umfassen alle anderen festen Serverrollen.
- Feste Serverrolle „SecurityAdmin" – Verwaltet Anmeldungen am Server.
- „Db_Owner" – Führt die Vorgänge aller Datenbankrollen sowie andere Wartungs- und Konfigurationsvorgänge in der Datenbank durch. Die Berechtigungen dieser Rolle umfassen alle anderen festen Datenbankrollen.
- „Db_AccessAdmin" – Fügt Gruppen und Benutzer von Windows NT® 4.0 oder Windows 2000 sowie SQL Server-Benutzer in der Datenbank hinzu oder entfernt diese.
- „Db_SecurityAdmin" – Verwaltet Rollen und Mitglieder von SQL Server 2000-Datenbankrollen sowie Anweisungs- und Objektberechtigungen in der Datenbank.
- „Db_BackupOperator" – Verfügt über Berechtigungen zum Sichern der Datenbank.

Unterstützen integrierte Produkte alle Sicherheitsfunktionen in Microsoft Dynamics GP?

Einige Sicherheitsfunktionen sind derzeit nicht auf alle zusätzlichen Produkte übertragbar. Diese werden jedoch höchstwahrscheinlich in zukünftigen Versionen hinzugefügt. Dies bedeutet, dass sich ein Administrator möglicherweise als Systemadministrator („sa") anmelden muss, um Tabellen zu initialisieren oder umzuwandeln, die eine Konvertierung erfordern. Damit zusätzliche Produktwörterbücher die Sicherheitsfunktionen nutzen können, wurde eine neue Funktion mit dem Namen „syUserInRole" erstellt, mit der ermittelt werden kann, welcher Datenbankrolle der Benutzer angehört.

In einer vorherigen Version von Microsoft Dynamics GP habe ich Berechtigungen festgelegt, indem ich den Zugriff auf bestimmte Paletten beschränkt habe. Was soll ich nun tun, da in Microsoft Dynamics GP keine Paletten mehr verwendet werden?

Da Zugriff auf Fenster, Berichte und Tabellen gewährt bzw. verweigert werden muss, wurden Benutzer durch die Zugriffsbeschränkung auf Paletten (in früheren Versionen als 8.0) lediglich davon abgehalten, auf die Fenster zuzugreifen, die mittels dieser Navigationsmethode verfügbar waren. Für diese Benutzer bestand weiterhin die Möglichkeit, mithilfe anderer Navigationsmethoden auf dieselben Fenster zuzugreifen (z. B. über die Shortcut-Leiste oder ein anderes Fenster, auf das Zugriff gewährt wurde). Der Zugriff auf die Informationen war ebenfalls über Berichte möglich oder über die Tabellen, in denen die Informationen mithilfe einer anderen Anwendung gespeichert waren. Daher sollten die Zugriffsrechte direkt für Fenster, Berichte und Tabellen gewährt bzw. verweigert werden und nicht über eine Beschränkung der Navigation.